AZƏRBAYCAN RESPUBLİKASI TƏHSİL NAZİRLİYİ

AZƏRBAYCAN DÖVLƏT İQTİSAD UNİVERSİTETİ (UNEC)

MAGİSTRATURA MƏRKƏZİ

Əlyazması hüququnda

ƏLİZADƏ LEYLA SALEH QIZI

"İNFORMASİYA TƏHLÜKƏSİZLİYİNİN HÜQUQİ TƏNZİMLƏNMƏSİNDƏ BEYNƏLXALQ TƏCRÜBƏ VƏ ONUN AZƏRBAYCANDA TƏTBİQİ"

mövzusunda

MAGİSTR DİSSERTASİYASI

İxtisasın şifri və adı: 060632 - "İnformasiya texnologiyaları və sistemləri mühəndisliyi"

İxtisaslaşma: "İnformasiya mühafizəsi və təhlükəsizliyi"

Elmi rəhbər: f.r.e.n., dos. T.Ə.ƏLİYEVA

Magistr proqramının rəhbəri: akad. Ə.M.ABBASOV

Kafedra müdiri: akad. Ə.M.ABBASOV

Bakı - 2020

MÜNDƏRİCAT **Səh.**

G İ R İ Ş

Tədqiqatın aktuallığı: İstər şəxsi informasiyanın, istər dövlət əhəmiyyətli informasiyanın digər üçüncü bir tərəfin əlinə keçməsi bütün dövrlərdə təbii olaraq insanları narahat etmişdir. İnformasiya mənbələrinin miqdarının kəskin artımı, İKT-nin sürətli inkişafı ilə əlaqədar olaraq, təhlükəsizliyin təmin olunması məsələsi də günbəgün aktuallığını artırmışdır. Müasir dövrümüzdə isə bu mövzu xüsusilə diqqət mərkəzindədir. Çünki, informasiya sistemlərinə olan təhdidlərin və hücumların sayında da böyük artım müşahidə olunur. İnformasiyanın dəyər aspekti baxımından nə qədər önəmli bir mövqedə durduğunu əsas götürsək, onun mühafizəsinin təmin olunması məsələsinin də əhəmiyyətini başa düşmək olar. Hal-hazırda ölkənin əsas sərvətlərindən biri kimi informasiya strateji əhəmiyyətli milli sərvət rolunu oynayır.

Problemin qoyuluşu və öyrənilmə səviyyəsi: Dissertasiya işində Azərbaycanda informasiya təhlükəsizliyinin hüquqi tənzimlənməsi sahasində görülən işlər, hüquqi bazanın üstünlükləri və çatışmazlıqları ətraflı şəkildə tədqiq olunmuşdur.

Tədqiqat işinin məqsədi: İnformasiya təhlükəsizliyi məsələsi keçmiş zamanlarda ayrı-ayrı ölkələrdə fərqli formalarda təşkil olunurdu. Buna görə də, çox zaman ayrı-ayrı dövlətlərin strategiyaları uyuşmurdu. Belə olan halda, ümumi bir qayda çərçivəsində razılaşmaqda müəyyən çətinliklər yaranırdı. Bu çətinliyi aradan qaldırmaq və ümumi prisiplərə əsaslanan qaydalardan istifadə etmək məqsədilə keçən əsrin sonlarında qanunlar toplusu – standartlar yaradılmağa başlandı. Bu standartlar vasitəsilə, artıq müttəfiq dövlətlərin hamısı “eyni bir dil”də danışmağa başlamışdılar. Qəbul olunmuş bu standartlardan ölkəmizdə də tətbiq olunur. Bu dissertasiya işində də ölkəmizdə bu standarların tətbiqi fonunda baş verən hadisələr, onların informasiya sistemlərinə təsirindən bəhs olunur.

Tədqiqatın predmeti və obyekti: Tədqiqat zamanı dünya praktikasında informasiya təhlükəsizliyinin tənzimlənməsinin hüquqi aspektləri, bu aspeklərin tarixi inkişaf yolu, hüquqi çərçivədə qəbul edilmiş standartlar, onların ölkəmizdə tətbiqi, əldə olunmuş nailiyyətlər və uğurlu siyasətdən bəhs olunur.

Tədqiqatın informasiya bazası və metodları: Hüquqi tənzimləmə mövzusunu araşdırarkən müxtəlif beynəlxalq sazişlərə, müqavilələrə və ayrı-ayrı ölkələrin qanunvericilik sisteminə nəzər salmaq lazım gəlir. Bu dissertasiya işində çoxsaylı elmi məruzələrdən və internet resurlarından istifadə olunmuşdur. Azərbaycanda informasiya təhlükəsizliyinin hüquqi tənzimlənməsi mövzusunun təqdiqi zamanı isə əsasən ölkədə əsas qanunverici baza olan Azərbaycan Respublikası Konstitusiyasına əsaslanıb. Bundan başqa, müxtəlif KİV-lərdə yer almış məqalələr, president.az veb saytındakı fərmanlar da informasiya bazası kimi qeyd olunub.

Tədqiqata uyğun elmi yeniliklər: Azərbaycanda informasiya təhlükəsizliyinin hüquqi tənzimlənməsi məsələsinin tədqiqi zamanı son illər bu sahəyə çox böyük diqqət və qayğının ayrıldığını görmək olur. Bu sahədə son dövrlərdə qüvvəyə minmiş onlarla qanun və fərman göstərir ki, gələcəyə yönəlmiş siyasətin bir parçası kimi, həqiqətən də, informasiya təhlükəsizliyi prioritet sahələrdən biri kimi qəbul olunub.

Tədqiqat işinin strukturu və həcmi: Dissertasiya işi giriş, 3 fəsil, nəticə və təkliflər və istifadə olunmuş ədəbiyyat siyahısından ibarətdir.

I Fəsildə informasiya təhlükəsizliyi anlayışı, onun əsas elementləri, əhatə dairəsi kimi anlayışlar geniş şəkildə izah olunmuş, informasiya təhlükəsizliyi siyasəti haqda məlumat verilmişdir. Həmçinin, təhlükəsizliyə yönəlmiş təhdidlər, onların geniş təsnifatı, qarşıya çıxa biləcək risklər və onların müxtəlif formaları haqda da ətraflı məlumat verilmişdir.

II Fəsildə təhlükəsizliyin təmini üçün əsas hüquqi üsullar şərh olunmuşdur. Hüquqi üsullarla yanaşı, bu fəsildə informasiya təhlükəsizliyi sahəsində beynəlxalq

təcrübə, dövlət siyasətləri, onların oxşar və fərqli xüsusiyyətləri, aralarındakı oxşarlıqlar, ziddiyyətlər də hərtərəfli tədqiq olunmuşdur.

III Fəsildə isə təqdiqatın əsas predmeti - Azərbaycanda bu sahədə beynəlxalq təcrübənin tətbiqi məsələsinə xüsusi yer verilmişdir. Ölkəmizdə bu sahədə baş verən əhəmiyyətli hadisələr, qəbul olunmuş qərarlar, qanunvericilik aktları və hal-hazırki şərait bu fəsildə tam tədqiq olunmuşdur.

Dissertasiya işi 3 fəsil və 8 paraqrafdan ibarət olmaqla 75 səhifə təşkil edir. İş yerinə yetirilərkən çoxsaylı ədəbiyyatlardan, xarici mənbələrdən və İnternet resurslarından istifadə edilmişdir.

I FƏSİL. İNFORMASİYA TƏHLÜKƏSİZLİYİ KONSEPSİYASI: ƏSAS ANLAYIŞLAR, TƏHLİL VƏ TƏHDİDLƏR

1.1. İnformasiya təhlükəsizliyi sisteminin quruluşu

İnformasiya öyrənmə, araşdırma və müşahidə yolu ilə əldə edilən hər cür faktlar, hadisələr və anlayışların cəmidir. Bu o deməkdir ki, ətrafımızdakı bütün hadisələr, obyektlər bizim üçün informasiya toplusu hesab oluna bilər. İnformasiya həmçinin, müəssisə və ya təşkilatın fəaliyyətini həyata keçirmək üçün istifadə etdiyi mənalı və faydalı məlumatlardır. İnformasiya bir qurumun davamlılığını və mövcudluğunu təmin edən yeganə amildir və təhlükəsizliyi mütləq təmin edilməlidir. Məhz bu səbəbdən informasiya təhlükəsizliyi anlayışı meydana gəlib.

İnformasiya təhlükəsizliyi (İT) informasiyanın həm saxlanıldıqda, həm də bir kompüterdən və ya fiziki yerdən digərinə ötürüldükdə icazəsiz girişdən və dəyişdirilmədən mühafizəsi üçün nəzərdə tutulmuş təcrübələr toplusudur. İnformasiya XXI əsrin ən vacib resurslarından birinə çevrildiyi üçün informasiyanın mühafizəsi üçün səylər də getdikcə daha vacib hala gəlmişdir.

İnformasiya təhlükəsizliyi yalnız icazəsiz girişdən informasiya əldə etməklə bağlı olan anlayış deyil. İnformasiya təhlükəsizliyi, əsasən, icazəsiz girişin, istifadənin, açıqlanmanın, pozulmanın, dəyişdirilmənin, yoxlanılmanın, qeyd edilmənin və ya məhv edilmənin qarşısının alınması təcrübəsidir. İnformasiya fiziki və ya elektrik siqnalı formasında ola bilər. İnformasiya sosial mediadakı profil, mobil telefondakı məlumatlar kimi şəxsi informasiyalar və ya biometrik verilənlər də ola bilər. İnformasiya təhlükəsizliyi informasiyanın təhlükəsizliyini və bütövlüyünü təmin edən və lazımi hallarda onu səlahiyyətli şəxslərin asanlıqla əldə etməsinə imkan verən sistemdir. İnformasiya Təhlükəsizliyi Sistemi (İTS) məlumatın icazəsiz istifadəsindən, icazəsiz açıqlanmadan, məhv edilmədən,

dəyişdirilmədən, məlumatın zədələnməsindən və ya icazəsiz əldə edilməsindən qorunma prosesidir. İnformasiya təhlükəsizliyi termini kompüter təhlükəsizliyi və informasiya sığortası terminləri ilə çox vaxt bir-birini əvəz edir. Çünki bu sahələr dövrümüzdə aktualdır və məxfiliyin, bütövlüyün və məlumatların əldə olunmasının mühafizəsində ümumi məqsədləri bölüşür. İTS Beynəlxalq ISO 27001:2013 standartı ilə tənzimlənir. Bu standartın tələblərini yerinə yetirən təşkilat dəyər aktivləri sırasında ən qabaqcıl mövqedə duran informasiya aktivlərinin təhlükəsizliyini təmin etmək üçün mühüm bir addım atmış hesab olunur. İTS standartı bütün növ təşkilatları (məsələn, kommersiya təşkilatları, ictimai qurumlar, qeyri-kommersiya təşkilatları və s.) əhatə edir. Bu standart təşkilatın bütün iş riskləri kontekstində sənədləşdirilmiş İTS-in yaradılması, tətbiqi, monitorinqi, nəzarəti, saxlanması və təkmilləşdirilməsi tələblərini əhatə edir. O həmçinin, müstəqil təşkilatların və ya tərəflərin ehtiyaclarına uyğunlaşdırılan təhlükəsizlik yoxlanışlarının aparılması tələblərini də müəyyənləşdirir.

İTS informasiya aktivlərini qoruyan və bu işdə marağı olan tərəflərə güvən verən adekvat və mütənasib təhlükəsizlik nəzarətini təmin etmək üçün hazırlanmışdır. İTS-in quraşdırılmasının üstünlükləri isə kifayət qədər çoxdur:

• İnformasiya aktivləri haqqında məlumatlılıq: Təşkilat informasiya aktivlərinin nə olduğunu və onun dəyərini dərk edir.

• Aktivləri qorumağı bacarmaq: İdarəetmə üsullarını və qorunma üsullarını müəyyənləşdirir və onları tətbiq etməklə aktivləri qoruyur.

• Biznesin davamlılığı: uzun illər təşkilatın işinə zəmanət verir.

• Əlaqəli tərəflərlə barışıqda olmaq: Əlaqədar tərəflərin etimadını qazanır, çünki informasiya, xüsusilə də onu təmin edənlər qorunmuş olur.

• İnformasiyanı bir sistem vasitəsi ilə qoruyur və şansa buraxmır.

• İşçilərin motivasiyasını artırır.

• Təqiblərin qarşısını alır.

• Yüksək nüfuz təmin edir.

Bu prinsiplərin bir təşkilata tətbiq olunması təhlükəsizlik siyasəti formasını alır. Bu təhlükəsizlik cihazı və ya proqram hissəsi deyil. Əksinə, müəssisənin

özünün xüsusi ehtiyaclarına və sorğularına əsasən məlumatların mühafizə formasını müəyyənləşdirən sənəddir. Bu siyasətlər kibertəhlükəsizliyin təmin edilməsi vasitələrinin alınması ilə bağlı təşkilatın qərarlarına rəhbərlik edir, həmçinin işçilərin davranışlarını və məsuliyyətlərini müəyyənləşdirir.

İnformasiya təhlükəsizliyindən bəhs edərkən ağıla 3 əsas element gəlir. Bu elementlər informasiya sisteminin etibarlı bir vəziyyətdə təhlükəsiz və bütövlüyünə zərər gəlməmiş bir iş şəraitində işləməsini təmin edir və informasiya aktivlərinin mühafizəsini təmin edən məxfilik, bütövlük və əlçatanlıq hesab olunur. Məxfilik, bütövlük və əlçatanlıq informasiya təhlükəsizliyinin əsasını təşkil edir. Bu üçlük qısaca CIA (**Confidentiality, Integrity, Availability)** adlanır. Bu elementlər əsasən aşağıdakılardır:

Məxfilik: Məxfilik bəlkə də informasiya təhlükəsizliyi barədə düşünəndə dərhal ağla gələn üçlüyün ilk elementidir. İnformasiyanın icazəsiz şəxslər və ya sistemlər tərəfindən əldə edilə bilməməsi və ya informasiyanın icazəsiz insanlara çatmasının qarşısının alınmasıdır. Həm kompüter sistemlərində işlənərkən, həm də şəbəkədə göndərici və qəbuledici arasında hərəkət edərkən informasiya icazəsiz girişdən qorunmalıdır. Təcavüzkar konfiqurasiya və ya proqram səhvindən istifadə edərək və ya Sosial Mühəndislik texnikaları ilə səlahiyyətli insanların səhvlərindən istifadə edərək icazəsiz informasiya əldə edə bilər. Bu prinsipdə nəzərə alınacaq məqam informasiyanın tamamilə gizlədilməsini təmin etmək deyil, onun icazəsiz alınmasının qarşısını almaq və əldə edilə biləcəyi zaman xəbərdar olmaqdır. Məsələn, mənim gmail hesabım üçün şifrəm var, amma mən gmail hesabına giriş edərkən bunu kimsə görürsə, bu halda şifrəm ələ keçir və məxfilik pozulur. Şifrələr, şifrələmə, identifikasiya və nüfuz hücumlarına qarşı qorunma məxfiliyi təmin etmək üçün hazırlanmış üsullardır. Məxfilik prinsipinin əsas anlayışlarını aşağıdakı kimi sadalamaq olar:

- *Sensitivity* - Həssaslıq
- *Discretion* - İstifadə
- *Criticality* - Tənqid

- *Concealment* - Gizlətmə
- *Secrecy* – Ümumi məxfilik
- *Privacy* – Şəxsi məxfilik
- *Seclusion* - Gizlənmə
- *Isolation* - İzolyasiya

Bütövlük: İnformasiyanın icazəsiz şəxslər tərəfindən dəyişdirilmək, silmək və ya məhv edilmək təhlükələrindən qorunmasıdır. Bütövlük üçün qısaca, təsadüfi və ya qəsdən məlumatın dəyişikliyə uğramaması kimi də ifadə edilə bilər. Burada məqsəd məlumatı olduğu kimi saxlamaq və qorumaqdır. Bu məqsədlə kritik məlumatlar üçün giriş nəzarəti aparılmalı və arxivləmə müəyyən fasilələrlə baş verməlidir. Bu prinsipdə diqqət yetirilməli məqam məlumatın dəyişdirilməməsini təmin etmək, icazəsiz dəyişdirilməsinin qarşısını almaq və dəyişiklik olduqda məlumatlandırılmadır. Bütövlük prinsipinin əsas anlayışlarını aşağıdakı kimi sadalamaq olar:

- Accuracy: Dəqiqlik
- Truthfulness: Doğruluk
- Authenticity: Orijinallıq
- Validity: Etibarlılıq
- Nonrepudiation: Təxirə salınmamazlıq
- Accountability: Hesabatlılıq
- Responsibility: Məsuliyyət
- Completeness: Tamlıü
- Comprehensiveness: Hərtərəflilik

Əlçatanlıq: İnformasiyanın ehtiyac olduğu halda istifadəyə hazır olduğunu bildirir. İnformasiyanın qorunduğu sistem üçün bir problem meydana gəldiyində və ya informasiya sisteminə yönəlmiş bir risk meydana gəlsə belə, informasiyanın əldə oluna bilməsi əlçatanlıq xüsusiyyətinin tələbidir. Bu giriş istifadəçinin

hüquqları daxilində olmalıdır. Əlçatanlıq prinsipinin diqqət yönəltdiyi amil istifadəçilərdir və hər bir istifadəçi səlahiyyət verilmiş müddətdə əlçatanlığı olan informasiya sisteminə daxil ola bilməlidir. Əlçatanlıq xidməti sayəsində istifadəçilər əldə olan imtiyazları daxilindəki informasiyanı informasiyanın təzəliyini itirmədən vaxtında və etibarlı şəkildə əldə edə bilirlər. Əlçatanlıq prinsipinin əsas anlayışlarını aşağıdakı kimi sadalamaq olar:

- Usability: Uyğunluq
- Availability: Mövcudluq
- Timeliness: Zamanlılıq

İdeal bir dünyada məlumatlar həmişə məxfi, düzgün, bütöv vəziyyətdə mövcud olmalıdır. Praktikada isə, hansı prinsipə daha çox üstünlük veriləcəyi haqda müəyyən seçimlər etməlisiniz. Məsələn, həssas tibbi məlumatlar saxlanılırsa, məxfiliyə diqqət yetirilir. Digər halda isə maliyyə qurumu heç kimin bank hesabına yanlış kredit verilməməsini təmin etmək üçün məlumatların bütövlüyünü əsas prinsip kimi vurğulamağı üstün tutur [1].

İnformasiya təhlükəsizliyi fərdi kompüterlərdən tutmuş, korporativ və milli səviyyədəki bütün informasiya sistemlərinə və kritik infrastrukturlara qədər geniş informasiya sistemlərini əhatə edən bir təhlükəsiz idarəetmə yanaşmasıdır. Korporativ səviyyədə informasiya sisteminin üçüncü tərəfi kimi informasiya sistemlərinə əlçatanlığı olan istifadəçiləri və informasiya sistemlərinə texniki dəstək verən proqram və ya aparat təminatçılarını göstərmək olar.

İT rəqəmsal arenada informasiyanın saxlanması və daşınması zamanı bütövlüyün pozulmadan, informasiyanın icazəsiz daxilolmalardan mühafizəsi üçün təhlükəsiz informasiya saxlama və emaletmə platforması yaratmaq üçün edilən səylərdir. Bunu təmin etmək üçün müvafiq təhlükəsizlik siyasəti təyin olunmalı və həyata keçirilməlidir. Bu siyasətlər fəaliyyətlərə nəzarət, girişi izləmək, dəyişikliklərin saxlanması və qiymətləndirilməsi və məlumatların silinməsinin məhdudlaşdırılması kimi bəzi üsullara əsaslana bilər. İnformasiya təhlükəsizliyi, ümumiyyətlə, təhlükəsizlik problemləri ilə ətraflı məşğul olan “təhlükəsizlik

mühəndisliyi”nin alt sahəsi kimi qəbul edilir. Şəkil 1-də qeyd olunduğu kimi, informasiya təhlükəsizliyi alt sahə olsa da, özünəməxsus xüsusiyyətləri ilə də seçilir.

Şək. 1. İnformasiya təhlükəsizliyi mühəndisliyin altçoxluğu kimi

Digər tərəfdən, informasiya təhlükəsizliyi geniş arealda kriptologiya, risklərin idarə edilməsi və təhlükəsizlik mədəniyyəti kimi fənlərlə əlaqədar olub, bunlar da informasiya təhlükəsizliyinin tərifində təbii olaraq əhatə olunmuş sahələr hesab olunur. İnformasiya təhlükəsizliyinin konseptual çərçivəsi kontekstində tez-tez istifadə olunan informasiya sistemləri və kritik infrastruktur kimi anlayışları da qeyd etmək faydalı olar.

İnformasiya sistemi informasiya texnologiyaları, istifadəçilərin qarşılıqlı əlaqəli olduğu və taktiki, inzibati və qərar qəbul etmə sistemi olaraq istifadə olunan sistemlərdir. Bu mənada, informasiya sistemi (İS) təkcə informasiya-kommunikasiya texnologiyaları (İKT) deyil, həm də iş proseslərini dəstəkləyən bu texnologiyalarla qarşılıqlı əlaqədə insanların onlardan istifadə yollarını da əhatə edir. Bu gün əsasən böyük miqyaslı kompüterlər əsasında fəaliyyət göstərir. Bununla yanaşı, rəqəmsal əsaslı İS-in işləməsi üçün kompüterlərdən başqa proqram təminatı, internet və dünya şəbəkəsi (www-dünya miqyaslı web) kimi aparıcılar, aparat, rabitə sistemləri də tələb olunur. Digər tərəfdən, fərdi

kompüterdən ən mürəkkəb superkompüterlərə qədər geniş diapazonu əhatə edən İS-də informasiyanın emalı, saxlanması və əldə edilməsini təmin etmək kimi funksiyalar mövcuddur.

Kritik informasiya infrastrukturları informasiya təhlükəsizliyi aspektindən xeyli vacibdir. Dünyadakı kritik infrastrukturların tərifinə dair hələ dəqiq bir fikir mövcud deyil, buna baxmayaraq, hər bir ölkənin öz şərtləri və ehtiyacları daxilində kritik infrastrukturun tərifi var. Lakin, kritik infrastrukturların ümumi xüsusiyyətləri araşdırıldıqda bir tərif vermək mümkündür.

Kritik infrastrukturlarda təhlükəsizlik tələblərinə cavab vermək yalnız müvafiq kritik infrastrukturun işləməsi üçün deyil, həm də sosial və iqtisadi inkişafın davamlılığı üçün zəruridir. Müasir dövrdə kritik infrastrukturun tərifi əvvəlki illərlə müqayisədə daha geniş məna daşıyır. Son illərdə media və mədəniyyət, internet xidməti təminatçıları (ISP) sektorlarının da artıq bir çox ölkələrdə kritik infrastruktur sektorlarından biri olduğu görünür. Bu anda diqqəti cəlb edən məqam, özəlləşdirmə səylərinin təsiri altnda ictimai həyat üçün vacib olan kritik infrastrukturların artan sürətlə özəl sektor qurumlarının nəzarətinə və idarəsinə verilməsidir. Xüsusilə ABŞ, Almaniya, İngiltərə, Yaponiya kimi kritik infrastruktur operatorlarının əksəriyyətinin özəl sektorda olduğu ölkələrdə beynəlxalq informasiya təhlükəsizliyi strategiyalarında dövlət-özəl əməkdaşlıq modellərinin yaradılması tendensiyası mövcuddur. Bu gün demək olar ki, hər bir beynəlxalq informasiya təhlükəsizliyi strategiyasının əsas prioritet məsələlərindən biri də kritik infrastrukturların qorunması və buna uyğun olaraq dövlət-özəl əməkdaşlıq modelinin yaradılmasıdır [2].

Son illərdə kiberhücumların ən vacib hədəflərindən birinə çevrilən kritik infrastrukturların qorunması yalnız sosial asayişi təmin etmək baxımından vacib deyil, eyni zamanda beynəlxalq inkişaf hədəflərinə çatmaqda və xidmət mərkəzində rolu olduğuna görə vacibdir. Bu məqsədlə kritik infrastrukturların mühafizəsi bu gün bir çox ölkələrdə milli informasiya təhlükəsizliyi strategiyalarının ayrılmaz və kritik bir elementi olaraq qəbul edilir. Hətta son

illərdə həm fiziki, həm də kibermühitdə kritik infrastrukturların qorunması üçün xüsusi milli strategiya və fəaliyyət planları hazırlayan ölkələrin sayı artır.

İnformasiya təhlükəsizliyi (İT) rəqəmsal və qeyri-rəqəmsal informasiyalara olan hücumların qarşısının alınması, aşkarlanması və sənədləşdirilməsi üçün zəruri olan proseslərin, alətlərin və siyasətlərin idarə olunması strategiyalarından ibarətdir. İT vəzifələri, məlumatın necə biçimləndiyindən və ya ötürülməsindən, işlənməsindən və ya saxlanılmağından asılı olmayaraq, informasiya aktivlərini qoruyacaq bir sıra iş proseslərinin qurulmasını əhatə edir. Həmçinin, İS-in fəaliyyətini həyata keçirərkən fasiləsiz, yüksək keyfiyyətli və etibarlı xidmət təqdim etmək məqsədi daşıyır. Digər tərəfdən, korporativ imicinin və etibarlılığının təmin edilməsi, informasiya aktivlərinin mühafizəsi və icazəsiz girişin qarşısının alınması İT-nin əsas vəzifələri və prioritetləri sırasındadır. Bir çox böyük müəssisə və təşkilatlar İT proqramını həyata keçirmək üçün xüsusi təhlükəsizlik qrupu işə götürür. Bu qrupa İT üzrə baş məmur rəhbərlik edir. Təhlükəsizlik qrupu ümumiyyətlə risk menecmentinin aparılmasına cavabdehdir. Bu zaman informasiya aktivlərinə olan həssaslıq və təhdid davamlı qiymətləndirilir və müvafiq qoruyucu qərarlar verilərək tətbiq olunur.

İT dörd mühüm vəzifəni yerinə yetirir:

- Təşkilatın fəaliyyət qabiliyyətini qoruyur.
- Təşkilatın informasiya təhlükəsizliyi sistemlərində tətbiq olunan tətbiqlərinin etibarlı işləməsini təmin edir.
- Təşkilatın topladığı və istifadə etdiyi informasiyaları qoruyur.
- Təşkilatın istifadə etdiyi texnologiyaya zəmanət verir.

İnformasiya təhlükəsizliyinin məğzi İS-in bütövlüyünə, məxfiliyinə və istifadəsinə hər hansı bir təhdidin aradan qaldırılmasından və bu təhdidlərin istifadə edə biləcəyi hər hansı bir təhlükəsizlik zəifliyinin aşkar edilərək həll olunmasından ibarətdir. Tərifinə görə sadə görünsə də, hücumların şaxələndirildiyi və mürəkkəbləşdiyi bir vaxtda İS-lərin təhlükəsizliyi getdikcə çətinləşir. Bu zaman

informasiya təhlükəsizliyi fəaliyyətinin effektiv olması üçün İS-lərə hansı risklərin və təhdidlərin yönəldiyini bilmək lazımdır.

1.2. İnformasiya təhlükəsizliyi siyasətinin sahələrinin tədqiqi

İnformasiya təhlükəsizliyinin qarşılıqlı əlaqəsi olan qeyri-məhdud sayda intizam və siyasət sahələri mövcuddur. Bunlara kompüter və şəbəkə təhlükəsizliyi, informasiya təhlükəsizliyinin idarə edilməsi sistemi, informasiya təhlükəsizliyinin idarə edilməsi, kriptologiya, kiber təhlükəsizlik, informasiya cinayətkarlığı, məlumatların məxfiliyi və mühafizəsi, milli təhlükəsizlik və beynəlxalq münasibətlər daxildir.

İnformasiya təhlükəsizliyinin kompüterlərə və şəbəkələrə tətbiqi nəticəsində şəbəkə və kompüter təhlükəsizliyi adlanan təhlükəsizlik anlayışı meydana gəldi. Kompüter və şəbəkə təhlükəsizliyi kompüterlərin informasiya sistemləri ilə və kompüterləri bir-birinə bağlayan şəbəkəyə aid aparat və proqram təminatı vasitəsilə icazəsiz giriş, sistemdəki məlumatların dəyişdirilməsinin və məhv edilməsinin qarşısını almaq üçün hər cür tədbir alınması kimi müəyyənləşdirilə bilər. Kompüter təhlükəsizliyi, həmçinin, informasiya sistemlərində qorunan məlumatların təbii fəlakətlər kimi gözlənilməz hadisələrə və fəlakətlərə qarşı tam və etibarlı şəkildə əlçatan qalmasını təmin edir.

Şəbəkə təhlükəsizliyi kompüter təhlükəsizliyindən texniki cəhətdən fərqli bir anlayışdır. Kompüter təhlükəsizliyi kompüterin daşıdığı informasiya sistemini risklərdən və hücumlardan qorumağa çalışdığından, şəbəkə təhlükəsizliyinin əsas məqsədi bir və ya bir neçə kompüterin bir-birilə informasiya mübadiləsi aparmaq, əlaqə qurmaq üçün istifadə etdiyi şəbəkəni hədəf ala biləcək icazəsiz girişlərə mane olmaq, bu şəbəkənin işini yerinə yetirməsinə əngəl ola biləcək hər cür amilləri təhlil edərək zərərsizləşdirməkdir. Şəbəkə təhlükəsizliyi bir tərəfdən şəbəkəyə girişi təmin etmək fəaliyyətləri həyata keçirərkən, digər tərəfdən də təhlükəsizlik təhdidlərinə qarşı qorunma və qarşısının alınması mexanizmlərini

təhlil edir və şəbəkəyə qarşı olan hücumların aşkarlanması və cavab mexanizmlərinin hazırlanmasını həyata keçirir.

Şəbəkə təhlükəsizliyi fərdi kompüterlərdən tutmuş korporativ informasiya sistemlərinə və hətta kritik informasiya infrastrukturlarına qədər hər bir informasiya sisteminin ehtiyac və imkanlarına uyğun olan tədbirlərin görülməsini tələb edir. Şəbəkənin ən effektiv istifadəsinin həyata keçirildiyi internet texnologiyalarının inkişafı ilə şəbəkə texnologiyalarının təhlükəsizliyini təmin etmək zərurəti, milli informasiya təhlükəsizliyi konsepsiyasından milli kibertəhlükəsizlik konsepsiyasına keçməyə böyük təsir göstərmişdir. Əslində, informasiya təhlükəsizliyi, kibertəhlükəsizlik və ya rəqəmsal təhlükəsizlik kimi istifadə olunan alternativ terminlərin hamısında ortaq bir nüans var: informasiya sisteminin təhlükəsizliyi.

İnformasiya texnologiyalarının geniş yayılması ilə informasiya texnologiyaları korporativ biznes proseslərinin bir hissəsinə çevrildi və informasiya sistemləri birbaşa korporativ hədəflərə çatmaq üçün bir vasitəyə çevrildi. Korporativ informasiya sistemlərinin informasiya təhlükəsizliyinin təmin edilməsi xüsusilə rəqəmsal mühitdə təhlükəsizlik risklərinin ortaya çıxmasından sonra vacib məsələ kimi qəbul edilmişdir. Korporativ idarəetmənin tərkib hissəsinə çevrilən informasiya sistemlərinin bütövlüyünün, məxfiliyinin və əlçatanlığının təmin edilməsi, informasiya təhlükəsizliyi idarəetməsi adlanan yeni idarəetmə modelinin yaranmasına səbəb oldu. Bu idarəetmə məntiqi bəzi müəlliflər tərəfindən informasiya təhlükəsizliyinin idarə edilməsinin üçüncü dalğa anlayışı kimi qəbul olunur. Birinci dalğa, informasiya texnologiyalarının istifadə olunduğu ilk dövrlərdə daha çox universal EHM-lər üçün nəzərdə tutulan idarəetmə modelidir. İnformasiya təhlükəsizliyi idarəetməsinin birinci dalğası olduqca yüksək texniki perspektivə malikdir. İkinci dalğa, qlobal şəbəkə texnologiyası tərəfindən internet və sonrakı e-ticarət texnologiyaları tərəfindən zərurət kimi yaradılmış informasiya təhlükəsizliyi menecmentinin qavranılmasıdır. İkinci

dalğada daha çox təşkilatların ən yüksək idarəetmə səviyyəsində informasiya təhlükəsizliyinin vacibliyini dərk etdiyi, lakin hələ də əsasən texniki həllini inkişaf etdirdiyi bir inkişaf müşahidə olunur. Üçüncü dalğa isə informasiya sistemlərinə olan təhdidlərin yalnız ikinci dalğa anlayışında olduğu kimi informasiya sisteminin idarəçiləri tərəfindən həll edilə bilməyəcəyini, bu risk və təhdidlərin idarəetmə, informasiya təhlükəsizliyi mədəniyyəti və vahid informasiya təhlükəsizliyi standartlarından birlikdə istifadə etməklə aradan qaldırıla biləcəyini nəzərdə tutur.

İnformasiya təhlükəsizliyi idarəetməsinin əsasları hər nə qədər ikinci dalğa dövrü adlandırılan 1990-2000-ci illəri arasında qurulsa da, üçüncü dalğa dövrü olan 2000-ci ildən bəri inkişaf etdiyini söyləmək olar. Üçüncü dalğadan əvvəl informasiya təhlükəsizliyinin təmin edilməsi yalnız bir sıra texniki standartların yerinə yetirilməsi və təşkilati dəstəyin yaradılması ilə mümkün olsa da, informasiya təhlükəsizliyi konsepsiyası informasiya sistemlərinin korporativ iş proseslərinin üçüncü dalğa ilə qarşılıqlı əlaqəsi nəticəsində korporativ məqsəd və strategiyaların bir hissəsi olmuşdur. Beynəlxalq informasiya təhlükəsizliyinin sertifikatlaşdırılması, informasiya təhlükəsizliyinin standartlaşdırılması, korporativ informasiya təhlükəsizliyi mədəniyyətinin formalaşması və davamlı və dinamik şəkildə informasiya təhlükəsizliyi baxımından informasiya sistemlərinin zəif və ya güclü cəhətlərinin ölçülməsi kimi bugünkü əsas anlayışlar informasiya təhlükəsizliyi ədəbiyyatına üçüncü dalğa ilə daxil oldu.

İnformasiya təhlükəsizliyi ilə sıx əlaqəli elm olan kriptologiya qədim zamanlardan bəri informasiyanı gizlətmə texnikası olaraq istifadə edilmişdir. Kriptologiyanın informasiya təhlükəsizliyinin təməl prinsipləri olan informasiyanın məxfiliyi, bütövlüyü, autentifikasiya prinsipləri ilə əlaqəli olduğunu söyləmək olar. Kriptologiya informasiyanın mühafizəsi, müəllif hüquqları ilə qorunan məhsulların məzmununa icazəsiz girişin məhdudlaşdırılması, xüsusən də internet texnologiyalarının yayılması ilə yeni istifadə sahələrini qazanmış oldu. Kriptologiya iki və ya daha çox ünsiyyət quran tərəfin təhlükəsiz

bir şəkildə informasiya mübadiləsinə imkan yaradan riyazi cəhətdən çətin ifadələrə söykənən bir sıra texnika və tətbiqlər toplusudur. Riyaziyyat, elektronika, optika, informatika, sosial mühəndislik elmləri kimi bir çox fəndən istifadə edən ixtisaslaşmış elmdir. Kriptologiya bəşəriyyətin yaranması ilə müxtəlif mərhələlərdən keçərək bu günə çatmışdır. Qısaca demək olar ki, bəşəriyyət yarandığı gündən kriptologiya da mövcud olub. Sadəcə, əvvəlcə insanlar yalnız məxfilik anlayışını həyata keçirmək üçün bu elmə ehtiyac duydularsa, artıq dövr dəyişdikcə kriptologiya şöbəsinin sahələri də dəyişir. Ənənəvi informasiya təhlükəsizliyinin tərkib hissəsi olan kriptologiya, müasir dövrlərdə xüsusən də informasiya sistemlərinə girişi məhdudlaşdırmaq üçün şifrəli mobil rabitə sahəsində, elektron poçt təhlükəsizliyinin təmin olunmasında, elektron imza kimi sahələrdə geniş istifadə olunan bir həll halına gəldi.

Kibertəhlükəsizliyi informasiya təhlükəsizliyinin altçoxluğu olan şəbəkə və kompüter təhlükəsizliyi anlayışının internetin inkişafından və yayılmasından sonra çevrildiyi yeni konseptual anlayış kimi göstərmək olar. Kibertəhlükəsizlik informasiya təhlükəsizliyinin altçoxluğu olsa da, son dövrlərdə ortaya çıxan beynəlxalq strategiya mətnlərində informasiya təhlükəsizliyi əvəzinə kibertəhlükəsizlik anlayışından istifadə edilə biləcəyi görülür. Kibertəhlükəsizliyə şəbəkələrə və informasiya sistemlərinə yönəlmiş kiberhücumların qarşısını almaq və kibercinayətkarlığa qarşı mübarizə daxildir. Digər tərəfdən, informasiya təhlükəsizliyi bir ölkənin informasiya aktivlərinin, kritik infrastrukturların, İKT infrastrukturunun, işgüzar və vətəndaşların biznes və əməliyyat təhlükəsizliyinin təmin olunduğu bir sosial-mədəni aspektə malik bir anlayışdır. Bu beynəlxalq informasiya təhlükəsizliyi ilə rəqəmsallaşdırılmış istənilən informasiyanın mühafizəsi və təhlükəsizliyini təmin etmək məqsədi daşıyır.

İnternetdəki bir çox mənbədə kiber təhlükəsizlik şəbəkə və kompüter təhlükəsizliyi ilə sinonim kimi istifadə olunur. Kibertəhlükəsizliyin ingilis dilində olan "cyber security" termini Vikipediyada axtarıldıqda “computer security”, yəni, kompüter və şəbəkə təhlükəsizliyinə yönləndirmə baş verir. Bu zaman

internetin inkişafından sonra kiber təhlükəsizlik anlayışının yalnız şəbəkə və kompüter təhlükəsizliyi ilə məhdudlaşdırmağın doğru olmadığını söyləmək olar. Çünki, kiberməkanın bugünkü sivilizasiyasını sosial və iqtisadi həyatı və asayişi hədəf alan qlobal təhlükəsizlik problemi ilə qarşı-qarşıya qoyduğunu müəyyən edən tədqiqatlar da mövcuddur.

İnformasiya cinayətkarlığı ilə informasiya təhlükəsizliyi və kiber təhlükəsizlik arasında sıx əlaqə var. İnformasiya sistemlərinə edilən hücumlara qarşı görüləcək texniki və prosedur tədbirləri toplusu İT daxilində olsa da, müxtəlif vasitə və metodlardan istifadə edərək bu informasiya sistemlərinə hücum edən cinayətkarlarla mübarizə kiber cinayət mövzusudur. Bu cinayətləri törədənlərin buraxdığı dəlillərin təqib edilməsi məhkəmə-ekspertiza sahəsinin vəzifəsidir. Kibercinayət internetdə yayılmış informasiya cinayətkarlığının xüsusi bir növü olaraq təyin edilə bilər. Cinayət hüququndakı tipik prinsipə uyğun olaraq, cinayət qanunda müəyyən edilmiş bir formada törədilməlidir. Bu zaman yeni hazırlanmış kibercinayətkarlıq növlərinin bəzilərinin tipik cinayət tərkibinə düşməməsi riski də var. Kibercinayətkarlıq anlayışı əvvəllər kompüter cinayətləri və ya şəbəkə cinayətləri kimi tanınırdı. Ancaq internet texnologiyalarının inkişafı nəticəsində kompüter cinayətkarlığı informasiya cinayətkarlığı olaraq tanınmağa başladı. Kibercinayətkarlıq anlayışı əslində informasiya cinayətkarlığın tərkib hissəsidir və onu internet texnologiyalarından istifadə etməklə həyata keçirilən kiber cinayət kimi müəyyən etmək olar.

İnformasiya cinayətkarlığının informasiya təhlükəsizliyinin əhatəsi ilə birlikdə qiymətləndirilməsi son dərəcə vacibdir, çünki təcavüzkarla mübarizə və hücumçunu mümkün hücumlardan çəkindirmək üçün təsirli bir vasitədir. Bu səbəbdən, demək olar ki, hər bir beynəlxalq informasiya təhlükəsizliyi strategiyasında informasiya cinayətlərinə qarşı mübarizənin alt komponenti mütləq daxil edilmişdir. Bunun ən vacib səbəbi internetin inkişafı ilə kiber cinayətlərin yayılması və bu cinayətləri cəzalandıran cəza qanunlarının qanunsuz cinayət anlayışı ilə bu cinayətlərin təsnifatı və hüquqi bazasında gecikdirilməsidir.

Şəxsi məlumatların mühafizəsi intizamı ilə informasiya təhlükəsizliyi və kibercinayətkarlıq bir-birilə əlaqəli hissələrdir. Xüsusilə, kibercinayətkarlıq, informasiyanın mühafizəsi qanunları və telekommunikasiya sahəsindəki tənzimləmələrlə beynəlxalq miqyasda yaradılan informasiya təhlükəsizliyi strategiyaları iç-içə keçmiş vəziyyətdə olduğundan informasiya təhlükəsizliyi ilə əlaqəli alınacaq siyasi tədbirlərin də mövcud telekommunikasiya, informasiya mühafizəsi və kibrcinayətkar siyasətindən asılı olmadan düşünülməməlidir. İnformasiyanın mühafizəsi qanunu adı verilən bu hüquq intizamı, bir informasiya sistemindəki şəxsi məlumat dəyərindəki məlumatların emalı, saxlanması və məhv edilməsi proseslərini özündə birləşdirən həyat dövrü içərisində bu məlumatlara yönəlmiş hər bir əməliyyatın səlahiyyətli şəxslər və əvvəlcədən təsdiqlənmiş qaydalar daxilində edilməsini təmin edən hüquqi və institusional quruluş modelidir. Şəxsi məlumatların sui-istifadə, icazəsiz işlənməsi və məhv edilməsi fərdi məlumatların saxlanıldığı informasiya sisteminə tamamilə kənar olan 3-cü tərəf hücumçular tərəfindən ediləbiləcəyi kimi sistemə giriş icazəsi olan, lakin onu sui-istifadə edən işçilər tərəfindən həyata keçirilə bilər. İnformasiya təhlükəsizliyi hər iki ssenaridə fərdi məlumatların icazəsiz istifadəsinin qarşısını almaq üçün bir sıra tədbirlər ortaya qoymuş olsa da, fərdi məlumatların, xüsusən də üçüncü tərəf hücumçular tərəfindən icazəsiz əllərə çatmasının qarşısını almaq məqsədi daşıyır. Bu hal fərdi məlumatların mühafizəsi ilə bağlı bir neçə qanuni mətndə əhatə olunur.

1.3. Təhlükəsizlik sistemlərinə olunan təhdidlərinin növləri

İnformasiya təhlükəsizliyi təhdidi dedikdə, sistemə və ya onun içərisində saxlanan məlumatlara arzuolunmaz təsir göstərə biləcək potensial hərəkətləri, hadisələri və ya prosesləri başa düşmək olar. İnformasiya və informasiya texnologiyalarının təhlükəsizliyinə əsas təhdid quldurlar və ya təcavüzkarlar tərəfindən edilən hücumlardır. Resurslara təsir göstərən bu cür təhdidlər

məlumatların pozulmasına, surətinin çıxarılmasına, icazəsiz paylanmasına, məhdudlaşdırılmasına və ya onlara girişin bloklanmasına səbəb ola bilər. Hal-hazırda müxtəlif meyarlara görə təsnif edilən kifayət qədər çox təhlükə məlumdur. Təbiidir ki, informasiya sistemlərindəki demək olarki, bütün təsnifatlar kimi bu təsnifat da müəyyən qədər şərti xarakter daşıyır, yəni, ayrı-ayrı ədəbiyyatlarda fərqli aspektlərə görə təsnifat görmək mümkündür.

Başvermə təbiətinə görə təbii və süni təhdidlər fərqlənir. Birinci qrupa obyektiv fiziki proseslərin və ya təbii fəlakətlərin kompüter sisteminə təsiri nəticəsində yarananlar daxildir. İkinci qrup - insan fəaliyyətindən qaynaqlanan təhdidlər kimi xarakterizə olunur.

Niyyətin təzahür formasına görə təhdidlər təsadüfi və qəsdən olaraq ayrılır. Həmçinin, onların bilavasitə mənbəyindən asılı olaraq təbii mühit, insanlar, sanksiyalaşdırılmış və sanksiyalaşdırılmamış aparat-proqram təminatı kimi bölgüsü var.

Təhdid mənbəyi fərqli mövqelərdə ola bilər. Bu amildən asılı olaraq üç qrup fərqlənir:

1. mənbəyi kompüter sisteminin idarə olunan qrupundan kənarda olan təhdidlər (nümunə olaraq, rabitə kanalları üzərindən ötürülən məlumatların tutulması)
2. mənbəyi sistemin idarə olunan zonasında olan təhdidlər (bu informasiya daşıyıcılarının oğurlanması ola bilər)
3. sistemin birbaşa özündə olan təhlükələr (məsələn, mənbələrdən düzgün istifadə edilməməsi).

Təhdidlər kompüter sisteminə müxtəlif yollarla təsir edə bilər. Bunlar passiv təhdidlər ola bilər, bir halda ki, onların həyata keçirilməsi məlumat strukturunun dəyişməsinə səbəb olmur, məsələn, surətin çıxarılmasını nümunə göstərmək olar. Aktiv təhdidlər isə, əksinə, kompüter sisteminin quruluşunu və məzmununu

dəyişdirən təhlükələrdir. Bu tip təhlükələrə isə xüsusi proqramların tətbiqini nümunə gətirmək olar.

İndi isə sadalananların ümumiləşmiş cədvəlinə nəzər salaq:

Təhdid və risklərin təsnifatı cədvəli

İşçi heyətdən irəli gələn risklər	**İnformasiya sistemindən qaynaqlanan risklər**	**Daxili proseslərdəki geriləmələr**	**Xarici amillərlə əlaqəli risklər**
1.1.Təsadüfi tədbirlər	2.1.Aparat təminatı riskləri	3.1.Prosesin dizaynı və ya həyata keçirilməsi ilə əlaqəli risklər	4.1.Təbii fəlakətlər
1.2.Qəsdən hərəkətlər	2.2.Proqram təminatı riskləri:	3.2.Proses nəzarətilə əlaqəli risklər	4.2.Hüquqi məsələlər
1.3.Passiv hərəkətlər	2.3.Sistemlə əlaqəli risklər	3.3.Dəstəkləmə prosesləri ilə əlaqədar risklər	4.3.İşlə əlaqəli məsələlər
			4.4.Nəqliyyat
			4.5.Xidmət asılılığı

İşçi heyətdən irəli gələn riskləri araşdıraq:

İS-in təhlükəsizliyini təhdid edən əməliyyat riskinin subyektləri olan şəxslər hərəkət edərək və ya hərəkətsiz qalmaqla səhlənkarlıq yolu ilə də risk yarada

bilərlər. Digər bir təsnifat əlaməti olaraq, riskin subyekti təşkilat daxilində və ya xaricində olan insanlar da ola bilər. Hər hansı bir əməliyyat nəticəsində risk baş verərsə, bu hərəkətlər qəsdən hərəkətlər və ya təsadüfi hərəkətlər kimi təsnif oluna bilər.

Təsadüfi hərəkətlərdə zərər vermək niyyəti olmur. Bu zaman şəxs zərərli sayılmır. Burada daxili səbəbləri xətalar, səhvlər və səhlənkarlıq kimi sıralamaq olar:

- Xəta: İşçilər düzgün proseduru bildiyinə və səy göstərməsinə baxmayaraq buna əməl edə bilməmişdirlər.
- Səhv: İşçilər düzgün proseduru bilmədikləri üçün buna əməl etməmişdirlər.
- Laqeydlik: işçilər nə edəcəyini bildikləri halda, səhlənkarlıq üzündən müraciət etməmişdilər.

Qəsdən hərəkətlərdə günahkar şüurlu şəkildə və zərər vermək niyyəti ilə hərəkət edir. Burada bu zərərli hərəkətin informasiya sisteminə vurduğu zərərə görə fırıldaq, təxribat, oğurluq və vandalizm şəklində növlər var.

- Fırıldaqçılıq: Özü və ya başqasının mənfəəti üçün təşkilatı risk və ya təhdid ilə qarşı-qarşıya buraxmaqdır.
- Təxribat: Bu informasiya aktivlərinə və ya informasiya sisteminə qəsdən ziyan vuran hərəkətə verilən addır. Təxribat, ümumiyyətlə, təşkilat daxilində elə bir şəxs tərəfindən həyata keçirilir ki, o şəxsin zədələnmiş aktivə giriş icazəsi olur. Bu giriş icazəsi həm təşkilat üzvündən, həm də müxtəlif informasiya sızması üsulları ilə də əldə edilə bilər.
- Oğurluq: İnformasiya sistemində mövcud olan informasiya aktivlərinə icazəsiz giriş vasitəsilə oğurlanma halıdır.
- Vandalizm: İnformasiya aktivlərinin əsasən təsadüfi və heç bir hədəf olmadan məhv edilməsinə verilən addır.

Passiv hərəkətlər informasiya sistemini qorumaq və ya idarə etmək məcburiyyətində olan şəxslərin məlumat və ya istedadının olmaması, əməliyyatlara nəzarət edən vəzifəli rəhbərin olmaması və ya müxtəlif başqa səbəblərdən yaranan informasiya təhlükəsizliyi riskləridir.

- İstedadın olmaması: İnformasiya təhlükəsizliyi üçün təhlükə və riski aradan qaldırmaq üçün fəaliyyət göstərən işçilərin istedad çatışmazlığı kimi müəyyən edilmişdir.
- Məlumatın azlığı: İşçi heyətin lazımi tədbirləri görmək üçün ehtiyac olan məlumata sahib ola bilməməsidir.
- Rəhbərliyin olmaması: Məsləhətçilərin düzgün tədbir görməsi üçün müraciət, idarəetmə və rəhbərlik proseslərindəki çatışmazlıqdır.

İnformasiya sistemindən qaynaqlanan risklərə aid olanlara nəzər salaq:

Sistem və texnologiyadan yaranan informasiya təhlükəsizliyi riskləri əməliyyat riskləri sırasındadır. Bu risklər texnologiyada gözlənilməz pozğunluqlar və ya zəifliklər kimi göstərilə bilər. Texnologiya ilə əlaqəli risklər isə aparat təminatı, proqram təminatı və inteqrasiya olunmuş sistemlərdə baş verə biləcək informasiya təhlükəsizliyi riskləridir.

Aparat təminatı (hardware) informasiya sistemini təşkil edən fiziki elementlərə verilən addır. Aparat təminatı riskləri dedikdə, informasiya sisteminin öz funksiyalarını yerinə yetirməsi üçün zəruri olan cihazın çatışmazlığı başa düşülür.

- Tutum: İnformasiya sisteminin imkanlarını aşan sərişdə tələb edən əməliyyat və proseslər nəticəsində yaranan risklər.
- Performans: İnformasiyanın emalı və ya saxlanması üçün tələb olunan sürət, enerji istehlakı, istilik yükü kimi parametrlərin əməliyyatın başa çatmasına mane olması.
- Texniki xidmət: Təchizatın tələb olunan və ya tövsiyə olunan istismar müddətində uğursuzluqlar.

- İstismar: Cihazın və ya aparatın xidmət müddətini ötməsi.

Proqram təminatı (software) informasiya sisteminin işləməsi üçün zəruri olan və aparat daxilində fəaliyyət göstərən xüsusi əmrlərdir. Adətən onlar proqram şəklində olurlar. Proqram bəzi çatışmazlıqlara malik ola bilər ki, məhz bu çatışmazlıqlar vasitəsilə də, informasiya sisteminə icazəsiz daxilolma mümkünləşər.

- Uyğunluq: Uyğunluqdan (compatibility) yaranan risklər ya informasiya sisteminin özündən, ya da bir neçə proqramın birlikdə işləməməsi nəticəsində yaranan risklərdir.
- Konfiqurasiya rəhbərliyi (Configuration management): sistemin konfiqurasiyası əməliyyatını təmin edən konfiqurasiya parametrləri təmin edilməməsidir.
- Dəyişiklik nəzarəti: tətbiqdə və ya onun konfiqurasiyasında meydana çıxan avtorizasiya problemləridir.
- Təhlükəsizlik parametrləri: Bir proqram və ya tətbiqdə lazımsız tezliklə səbəb olduğu məsələlərdir.
- Kodlaşdırma: Alqoritm və ya məntiq səhvləri səbəbindən proqram kodlaşdırmasında yaranan zəifliklərdir.
- Test: Bunlar bir proqramın tətbiqi və ya konfiqurasiyasında qeyri-adekvat və ya uyğunsuz sınaqların aşkarladığı təhlükəsizlik riskləridir.

İS-in dizaynındakı, sistem alqoritmidəki məntiqi səhvlər, informasiya sisteminin başqa bir sistemlə inteqrasiyası zamanı meydana çıxan təhlükəsizlik çatışmazlıqları və dizayn səhvləri sistemlə əlaqəli risklər sayılır.

- Dizayn riskləri: sistemin istifadəsində baş verən dizayndan irəli gəlir risklər.
- Texniki şərtlər: Sistem əvvəlcədən dizayn edildiyi zaman istifadəyə uyğun olmayan təsvirlər.
- İnteqrasiya riski: Sistemi işlək vəziyyətə gətirən əsas komponentlərin arasında birləşmənin pozulması problemi.

- Qarışıqlıq: Sistemlərdəki sektorlar və ya tətbiq modulları arasında lazımsız və həddindən artıq əlaqələr, alqoritmik səhvlər.

Sistem və texnologiyadakı uğursuzluqlar əməliyyat riskləri adlanır. Bu risklər informasiya sisteminin düzgün işləməsinə mane olan gözlənilməz və qeyri-adi əngəllərdir. Çox vaxt onlar proqram təminatı, aparat təminatı və inteqrasiya olunmuş sistemlərdə görülən qüsurlardır. Bu cür uğursuzluqlar informasiya sisteminin təhlükəsizliyinə risk hesab olunur. Məsələn, informasiya sisteminin iş prosesindəki məsuliyyəti və rolu tam müəyyənləşdirilməmiş olması, nəzarət və yoxlamanın olmaması, təsirsiz dəstəkləmə prosesləri daxili prosesdəki uğursuzluqlardır.

Prosesin dizaynı və ya həyata keçirilməsi ilə əlaqəli risklər bu prosesin əmələ gətirəcəyi nəticəni əldə etmək üçün tələb olunan vaxtın ortaya çıxardığı riskdir. Proses dizaynının və həyata keçirilməsinin əsas elementləri kimi proses axını, proses sənədləri, rol və məsuliyyət, bildiriş və siqnallar, informasiya axını, problemlər toqquşması, xidmət səviyyəsi razılaşmaları, tapşırıq dəyişiklikləri və s.-ni saymaq olar.

Proses nəzarətilə əlaqəli risklər proses nəzarəti ilə əlaqəli risklər əməliyyat sisteminin əməliyyat proseslərində idarəetmənin olmamasından yaranan riskdir. Bu risklər sistem proseslərinin uğursuz olmasına və ya tamamilə dayandırılmasına səbəb ola bilər. Proses nəzarətinin alt elementləri monitorinq, ölçmə və dövri nəzarət və proses mülkiyyətidir.

Dəstək prosesləri olaraq təyin olunan əməliyyat risklərinin alt şöbəsi, informasiya sistemini idarə edən şəxs və ya təşkilatın yetərli olmayan resurslarla dəstəklənməsi və ya ümumiyyətlə resusların olmaması kimi göstərilə bilər. Dəstək prosesləri ilə əlaqəli informasiya təhlükəsizliyi riskləri əsasən kadr, uçot, təlim və inkişaf və təchizat prosesləri zamanı baş verir.

Xarici amillər və ya hadisələr informasiya sistemini idarə edən şəxsin və ya təşkilatın nəzarəti xaricində baş verən hadisələr kimi müəyyən edilir. Bu cür tədbirlərin yeri, vaxtı və ya forması heç vaxt planlaşdırıla və ya proqnozlaşdırıla bilməz. Fəlakətlər, hüquqi məsələlər, biznes riskləri və xidmət asılılığı xarici amillər sayıla bilər [3].

II FƏSİL. İNFORMASİYA TƏHLÜKƏSİZLİYİNİN HÜQUQİ TƏNZİMLƏNMƏSİ

2.1. İnformasiya təhlükəsizliyinin təmini üçün əsas hüquqi üsullar

İnformasiya təhlükəsizliyini təmin etməyin bir neçə metodu var ki, bunlar qoruma üsulları adlanır [4]:

- Fiziki və proqram təminatı vasitəsi ilə iddia edilən müdaxilə üçün maneə.
- İdarəetmə və ya qorunan sistemin elementlərinə təsir.
- Kriptoqrafik metodlardan istifadə etməklə informasiyanın dəyişdirilməsi.
- Tənzimləmə və ya qanunvericiliyin inkişafı və verilənlər bazası ilə işləyən istifadəçiləri düzgün davranışlara təşviq etməyə yönəlmiş tədbirlər.
- İstifadəçinin məlumatların işlənməsi qaydalarına riayət etmək məcburiyyətində qalması üçün şəraitin yaradılması.
- İstifadəçiləri düzgün davranmağa sövq edən bir mühitin qurulması.

İnformasiya təhlükəsizliyinin aşağıdakı səviyyələri var:

1. İnzibati - Təşkilatın rəhbərliyi tərəfindən yerli səviyyədə alınmış bir sıra tədbirlər;
2. Prosessual səviyyə - İnsanların həyata keçirdiyi təhlükəsizlik tədbirləri;

3. Proqram təminatı və texniki səviyyə - Birbaşa informasiya təhlükəsizliyi vasitələri.
4. Qanunvericilik - Beynəlxalq ictimaiyyətin qanunları, qaydaları və digər sənədləri;

İnzibati səviyyədə təhlükəsizlik mütəxəssisləri çox vaxt aşağıdakı öhdəlikləri götürür:

- Kompüter avadanlıqları və məxfi məlumatlarla işləmə qaydalarını müəyyən edən daxili sənədlər hazırlayır;
- Kadrlarda dövri yoxlamalar aparır;
- İşlə bağlı məlumatların açıqlanması və ya sui-istifadəsi üçün məsuliyyətləri müəyyənləşdirən əmək müqavilələrinə əlavə müqavilələrin imzalanmasına təşəbbüs göstərir;
- Bir işçinin ən vacib məlumat sənədlərinin ixtiyarında olduğu halların qarşısını almaq üçün məsuliyyəti bölüşdürür; ümumi iş axını tətbiqetmələri ilə işi təşkil edir və kritik sənədlərin şəbəkə disklərində saxlanılmasını təmin edir;
- Məlumatları hər hansı bir istifadəçi, o cümlədən şirkətin üst rəhbərliyi tərəfindən surətinin çıxarılması və ya məhv edilməsindən qoruyan proqram məhsullarını təmin edir.
- Hər hansı bir səbəbdən uğursuz olduqda sistemin bərpa planlarını hazırlayır.

Texniki səviyyədə təhlükəsizliyin təmin olunması zamanı aparat və proqram təminatı birləşdirilir. Burada əsas vəzifələr:

- Kompüter sistemindəki ən vacib məlumat fayllarının müntəzəm olaraq ehtiyat nüsxəsinin saxlanması;
- Məlumatların təhlükəsizliyi üçün vacib olan bütün şəbəkə altsistemlərinin nüsxəsi və ehtiyat nüsxəsinin alınması;

- Fərdi elementlərin nasazlığı halında şəbəkə mənbələrini yenidən bölüşdürmək imkanı;
- Ehtiyat enerji təchizatı sistemlərindən istifadə etmək imkanı;
- Yanğından və ya suyun verdiyi zərərdən təhlükəsizliyin təmin edilməsi;
- Verilənlər bazaları və digər məlumatları icazəsiz girişdən qoruyan qabaqcıl məhsulların quraşdırılması.

İnformasiya təhlükəsizliyi sisteminin qanunvericilik səviyyəsinin qurulması isə əsas şərtlərdən biri hesab olunur. Çünki, bu mövzunun əsas konsepsiyalarını təmin edir və potensial təhdidlər üçün cəzanı müəyyənləşdirir. Bu səviyyə koordinasiya və rəhbərlik rolunu oynayır və informasiya təhlükəsizliyini pozan insanlara qarşı mənfi və cəzalandırıcı münasibətin qorunmasına kömək edir.

Qanunvericilik səviyyəsi haqqında danışarkən, ilk öncə tarixi xronologiyaya nəzər yetirmək lazımdır. Çünki, qısa zaman kimi görünsə də, bu sahədə əldə olunan nailiyyətlər kifayət qədər çoxdur.

Texnoloji tərəqqi müasir dünyada qısa zaman ərzində köklü dəyişikliklərə səbəb oldu. Belə ki, çox qısa zaman ərzində beynəlxalq münasibətlər sistemi dəyişmiş, İKT-nin inkişafı ictimai həyatın bütün sahələrinə, o cümlədən - iqtisadiyyat, siyasət, sosial elmlər və mədəniyyətə təsir göstərərək onları informasiya cəmiyyətinin qurulması çərçivəsində bir araya gətirdi. İndiyə qədər informasiya cəmiyyəti anlayışı bir çox beynəlxalq sənədlərdə qeyd olunub. Bunların arasında "İnformasiya Cəmiyyətinin yaradılması: Yeni minillikdə qlobal çağırış" Prinsiplər Bəyannaməsi (bir çox mənbədə bu sənəd 2003-cü il Bəyannaməsi kimi də adlanır) və İnformasiya Cəmiyyəti üzrə Dünya Sammitinin 12 dekabr 2003-cü il tarixli Tədbirlər Planı əsas sənədlər kimi xüsusi əhəmiyyətə malikdir.

İnformasiya cəmiyyəti qlobal informasiya cəmiyyəti ilə müqayisədə daha ümumi bir kateqoriyadır. Bu tək bir dövlət daxilində, regional və ya qlobal

səviyyədə də qurula bilər. Qlobal səviyyədə onu qlobal informasiya cəmiyyəti adlandırırlar.

Qlobal informasiya cəmiyyəti - beynəlxalq informasiya münasibətlərinin siyasi, iqtisadi, sosial və mədəni əlaqələrə təsir göstərən, İKT-yə əsaslanan informasiya sistemlərinin istismarı sahəsində qurulan beynəlxalq münasibətlər sistemi kimi təyin edilə bilər. Eyni zamanda, dövlətlər beynəlxalq informasiya münasibətlərinin bərabər subyektləri kimi qlobal informasiya cəmiyyətindəki münasibətlərdə də iştirak edirlər.

İKT-nin inkişafı beynəlxalq hüququn təsis edilmiş filiallarına və institutlarına təsiri və həmçinin, İKT-nin inkişafı nəticəsində yaranan yeni münasibətlərin tənzimlənməsi ilə əlaqədardır. Ən mürəkkəb problem İKT-nin qurulmuş beynəlxalq hüquq institutlarına təsiri ilə bağlıdır. Beynəlxalq hüquq müddəalarının inkişafı mexanizmi belədir ki, hüquqi tənzimləmələr İKT-nin inkişaf səviyyəsindən "geri qalır".

Hal-hazırda İKT-nin inkişafı və istifadəsi bütün beynəlxalq birliyin maraqlarına təsir göstərir. Bu texnologiyalar potensial olaraq beynəlxalq sabitlik və təhlükəsizlik məqsədlərinə uyğun olmayan məqsədlər üçün istifadə edilə bilər və beləliklə, mülki və hərbi sahələrdə təhlükəsizliyi pozaraq dövlətlərin infrastrukturunun bütövlüyünə mənfi təsir göstərə bilərlər. Beynəlxalq informasiya təhlükəsizliyini təmin etmək üçün ayrı-ayrı dövlətlərin səyləri kifayət deyil. Əvvəla, dövlətlərin informasiya silahından istifadəsinə qadağa beynəlxalq hüquqda təsis edilməlidir. Fərdi şəxslərin informasiya təhlükəsizliyi məsələləri üçün isə ayrıca tənzimləmə tələb olunur.

Beynəlxalq informasiya hüququnun formalaşdırılması prinsiplərinə İKT-dən istifadə zamanı məxfilik və təhlükəsizlik prinsipi daxildir. İnformasiya təhlükəsizliyi və şəbəkə təhlükəsizliyi, identifikasiya, məxfilik və istehlakçı müdafiəsi də daxil olmaqla etimad çərçivəsinin gücləndirilməsi informasiya cəmiyyətinin inkişafı və İKT istifadəçiləri arasında etimadın möhkəmlənməsi üçün vacib şərtdir. Qlobal kiber təhlükəsizlik mədəniyyətini bütün maraqlı tərəflər və beynəlxalq ekspert qurumları ilə birlikdə tanıtmaq, inkişaf etdirmək və tətbiq

etmək lazımdır. Bu səylər həmçinin, günü-gündən artan beynəlxalq əməkdaşlıqla dəstəklənməlidir. Bu qlobal kiber təhlükəsizlik mədəniyyətində təhlükəsizliyi artırmaq, girişi və ticarəti artırarkən məlumatların və məxfiliyin qorunmasını da təmin etmək vacibdir.

2003-cü il tarixli Bəyannamədə "kiber təhlükəsizlik" termini daha çox kiber cinayətlərdən qorunma mənasını daşıyır. Xüsusilə, Bəyannamədə qeyd olunur ki, sammit iştirakçıları BMT-nin İKT-nin beynəlxalq sabitliyin və təhlükəsizliyin qorunması məqsədlərinə zidd olan və dövlətlər daxilindəki infrastrukturun bütövlüyünə mənfi təsir göstərə biləcək və təhlükəsizliyinə zərər vuracaq məqsədlər üçün istifadəsinin qarşısının alınması üçün fəaliyyətlərini dəstəkləyirlər.

Bu qaydalar beynəlxalq informasiya hüququnun inkişaf edən prinsipinin mövcud prinsiplərlə, yəni fikir, ifadə və məlumat azadlığının həyata keçirilməsinin sülhün və beynəlxalq təhlükəsizliyin möhkəmləndirilməsində vacib amil olması ilə əlaqəsini təmin edir. Bu zaman bir neçə prinsipə də xüsusi diqqət yetirilir:

- medianın sülhün və beynəlxalq sazişlərin möhkəmlənməsinə və irqçiliyə, irqi ayrıseçkiliyə və müharibə təhrikinə qarşı mübarizəyə töhfə verməsi prinsipi;
- yayılması sülhün və beynəlxalq razılıqların möhkəmləndirilməsinə, insan hüquqlarının inkişafına, irqçiliyə, irqi ayrıseçkiliyə və müharibəyə təhrikə qarşı mübarizəyə xələl gətirən məlumatların təkzib edilməsini ictimailəşdirməyin vacibliyi prinsipi.

Fiziki və hüquqi şəxslərin informasiya təhlükəsizliyi problemləri Bainbridge, Campbell, Rowland and Macdonald, Smedinghoff və Black kimi alimlər tərəfindən informasiya texnologiyalarının müqayisəli qanununa dair fundamental tədqiqatlarda araşdırılmışdır. İnformasiya təhlükəsizliyinin təmin edilməsinin texniki və təşkilati aspektləri isə Egan və Mather, Hunter, Volonino və Robinson öz əsərlərində işıqlandırılmışdır.

Beynəlxalq informasiya təhlükəsizliyinin təmin edilməsi konsepsiyasının həyata keçirilməsi məsələsi konsepsiyanın özünün nəzərdə tutulmamasına

baxmayaraq, tədqiqatda artıq nəzərdən keçirilmişdir. Lloyd, ilk növbədə, "yumşaq qanun" aktlarına baxaraq məxfilik məsələlərini həll edərkən BMT, Avropa Şurası, OECD (Organisation for Economic Co-operation and Development - İqtisadi İnkişaf və Əməkdaşlıq Təşkilatı) və Avropa Birliyinin aktlarını nəzərə aldı. Kiber cinayətkarlıq problemlərinə dair bir araşdırmada bu müəllif Avropa Şurasının Kibercinayətkarlıq haqqında Konvensiyasına, İnformasiya Sistemlərinin Təhlükəsizliyinə dair OECD Təlimatlarına xüsusi diqqət yönəltmişdir [11].

23 noyabr 2001-ci il tarixli Kibercinayətkarlıq haqqında Konvensiyanın məzmunu və əhəmiyyəti Lloyd, Murray və Koops, Prins və Schellekens tərəfindən aparılan tədqiqatlarda müzakirə edilmişdir. Lakin bu tədqiqatlar Avropa Şurasının təcrübəsindən qlobal səviyyədə istifadə problemlərini əhatə etməyib.

2001-ci il Konvensiyasına gəldikdə isə, Hopkins əsas şərtlərin həddindən artıq geniş və aydın olmamasını vurğulamışdır. Məsələn, bu Konvensiya kompüter sistemini hər hansı bir cihaz, bir qrup cihaz və ya əlaqəli qurğular kimi müəyyənləşdirir ki, bunlardan biri proqrama uyğun olaraq informasiyanın avtomatik işlənməsini həyata keçirir. Buna görə 2001-ci il Konvensiyasının əhatə dairəsi həqiqi kompüter cinayətlərindən proqram təminatının istifadə olunduğu istənilən cihazlara müdaxiləyə qədər genişləndirildi. Beynəlxalq aktlarda fərdi məlumatlar anlayışı hüquqi doktrinada tənqid edilmişdir. Xüsusilə, Berčiç və George bu tərifin çox geniş olduğunu bildirirlər, çünki, bir şəxs haqqında hər hansı bir məlumat şəxsi məlumat kimi qəbul edilə bilər. Digər tərəfdən, müəyyən məlumatların şəxsi məlumatlar kimi qeyd edilməsi ilə bağlı praktik çətinliklər yaranır.

Polcak Avropanın müxtəlif ölkələrində IP ünvanlarını, fərdi telefon nömrələrini, İnternet üzərindən xidmət alarkən anonim olaraq daxil edilmiş məlumatları və ölən şəxslərin məlumatlarını fərdi məlumatlar olaraq qeyd etməkdə çətinliklərin olduğunu da qeyd etmişdi.

Milli qanunvericilik sistemlərində fərdi məlumatların vahid siyahısının olmaması beynəlxalq hüquqi tənzimləmənin təkmilləşdirilməməsinin səbəbidir. Məhz bu səbəbdən, uyğunlaşma sahəsində görülən işlər kifayət qədər uğurlu alınmadı. Bu, şəxsi məlumatların öz tərifini yaratmaq üçün milli səviyyədə edilən cəhdlərlə də təsdiqlənmiş olur.

Hazırda qlobal beynəlxalq müqavilələrin qəbul olunması təklifləri ilk növbədə qeyri-dövlət iştirakçılarından gəlir. 2000-ci ilin avqustunda Stenford Universitetinin bir qrup tədqiqatçısı kiber cinayət və terrorizmdən qorunmanın gücləndirilməsi üçün beynəlxalq konvensiyanın layihəsini (Stanford Layihəsi) təqdim etdi. Braun silahlı münaqişələrdə informasiya sistemlərinin istifadəsini tənzimləyən bir konvensiya hazırladı. 6 Noyabr 2009-cu ildə Beynəlxalq İnformasiyaların Mühafizəsi və Məxfilik Komissarlarının Konfransı "Məxfilik və Fərdi Məlumatlar Standartları" adlı qətnamə qəbul etdi, bunun üçün qlobal müqavilə layihəsinin hazırlanması üçün işçi qrupu yaradıldı və onun hazırlanması meyarları verildi. Müqavilənin hazırlanmış hissələrini BMT-yə təqdim etmək planlaşdırılmışdı. Beləliklə, tədqiqatçılar və beynəlxalq forumlar konkret layihələr təklif etmiş, lakin BMT, Beynəlxalq Telekommunikasiya İttifaqı (İTU) və ya UNESCO çərçivəsində heç bir sistemli iş aparılmamışdır [5].

Hətta, bu sahədə regional və qlobal səviyyələri və onun hüquqi bazasının inkişafı problemlərini əhatə edəcək beynəlxalq informasiya təhlükəsizliyinin ümumi konsepsiyasının monoqrafik tədqiqatları da mövcud deyil. Bu isə bir daha göstərir ki, müasir dövrümüzdə belə bu sahə hələ də tam tədqiq edilməmiş və lazımi qərarlar qəbul olunmamışdır.

2.2. İnformasiya təhlükəsizliyinin hüquqi təminatı sahəsində beynəlxalq təcrübə

Qlobal İnformasiya Təhlükəsizlik Statistikalarına nəzər salmaq məsələnin nə dərəcədə ciddi olduğunu anlamağa kifayət edir.

Bu günə qədər baş verən hadisələr və narahatlıqlar bizə müəyyən qədər gələcəyi görməyə imkan verir və illər irəlilədikcə vəziyətin pisləşəcəyini görmək heç də çətin deyil. Təhlükəsizliyə dair sığorta xərclərinin 2022-ci ilə qədər 14 milyard ABŞ dollarına qədər artırılması gözlənilsə də, bizneslərin 68%-i ümumiyyətlə, heç bir öhdəlik daşımır. Müəssisələrin 80%-də isə təhlükəsizliyin qarşısının alınması və təsirini azaltmaq üçün hərtərəfli plan mövcud deyil.

Qlobal olaraq, ən həssas sektorlardan biri 2015-ci ildə səhiyyə sahəsidir. Səhiyyə sahəsi ən çox xərc tələb edən yeddi səbəbdən üçündən zərər çəkmiş sahə hesab olunur. Onun ardınca ikinci yerdə istehsal sahəsi dayanır, bank-maliyyə sənayesi isə ilk üçlüyü tamamlayır.

Hücumlar və istismarlar isə gün keçdikcə mürəkkəbləşir və onları aşkar etmək çətinləşir. Araşdırmalar göstərir ki, hər 39 saniyədə bir hücum cəhdi olur. Bu hücumların yarıdan çoxu kiçik biznesə yönəlmişdir. Təkcə keçən il kiber cinayətkarlar tərəfindən yarım milyarddan çox şəxsi sənəd oğurlandı. Hesablamalara görə, gələcək 10 ildə bir məlumat pozuntusunun orta dəyəri təxminən 150 milyon dollara çatacaq.

Hər hansı bir dövlətin informasiya təhlükəsizliyinin qanunvericilik bazasının inkişafı və təkmilləşdirilməsi həyatının sosial-iqtisadi, siyasi, hərbi sahələrinin inkişafında məlumatların qorunmasına ehtiyacı təmin edən zəruri tədbirdir. İnformasiyanın qorunması sahəsində ilk hüquqi aktlar dövlət sirrinin qorunması haqqında qanunlar idi.

ABŞ-ın "İnformasiya təhlükəsizliyinin idarə edilməsi haqqında" 2002-ci il tarixli Qanununda informasiya təhlükəsizliyi aşağıdakı kimi xarakterizə edilir:

- informasiyanın və informasiya sistemlərinin icazəsiz girişdən, istifadədən, yayılmadan, dəyişdirilmədən və ya məhv edilmədən müdafiəsi;

- həqiqiliyinin təminatları da daxil olmaqla, informasiyanın tamlığının qanunsuz dəyişdirilmədən və ya məhvedilmədən mühafizəsinin təmin edilməsi;
- şəxsi həyat və mülkiyyət haqqında məlumatların gizliliyi də daxil olmaqla, tanış olma və yayılma imkanları məhdudlaşdırılmış informasiyanın konfidensiallığının təmin olunması;
- informasiya ilə tez və etibarlı şəkildə tanış olma imkanını ifadə edən əlçatanlıq.

İndiyə qədər bütün inkişaf etmiş ölkələrdə casusluq və xəyanət ən ağır cinayət sayılır. Avropada hələ də qüvvədə olan ən qədim qanunlardan biri XIX əsrin sonu - XX əsrin əvvəllərində dərc edilmiş Fransanın Cəza Qanunu məcəlləsidir. Bu qanun xəyanət forması kimi casusluğa görə cəzanı nəzərdə tutur. XIX əsrin sonlarında demək olar ki, bütün aparıcı Avropa ölkələri casusluq əleyhinə qanunlarını qəbul etmişdilər (1870-ci ildə Almaniyada, 1889-cu ildə İngiltərədə, 1890-cı ildə İtaliya və s.). Hal-hazırda da beynəlxalq səviyyədə geniş sosial əhəmiyyətə malik olan, cəmiyyət üçün ən dəyərli, həyati əhəmiyyətli bir qaynaq olaraq informasiya üzərində sabit bir fikir formalaşmışdır.

İnformasiya təhlükəsizliyinə hüquqi dəstəyin verilməsində beynəlxalq təcrübənin təhlili göstərir ki, dünya birliyində bu problemin inkişafı əsasən aşağıdakı sahələrdə aparılır:

- informasiya sahəsində fərdi hüquqların qorunması;
- dövlət maraqlarının qorunması;
- biznes və maliyyə fəaliyyətinin qorunması;
- məlumatların kompüter cinayətlərindən qorunması.

İnformasiya sferasında fərdi hüquqların mühafizəsi dünya birliyi üçün yeni deyil. Şəxsi həyata müdaxilənin dövlət və digər qurumlar tərəfindən məhdudlaşdırılmasının əsas prinsipləri fundamental normalarla müəyyən edilir. Bu

normalara İnsan Hüquqları Bəyannaməsi, BMT Konvensiyası və Avropa Şurasının İnsan Hüquqları Konvensiyasını nümunə göstərmək olar. Bu sahədə Qərb ölkələrinin qanunvericiliyi üç əsas istiqamətdə inkişaf edir [6]:

I istiqamət:

Şəxsin məlumat əldə etmək hüquqlarının qorunması, onun alınması və paylanması. Bu istiqamətdə ən vacib addım 1948-ci il dekabrın 10-da BMT Baş Assambleyası tərəfindən Ümumdünya İnsan Hüquqları Bəyannaməsinin qəbul edilməsi və elan edilməsi idi. Bu Bəyannamənin 19-cu maddəsində göstərilir: "Hər kəsin düşüncə və fikir azadlığı hüququ vardır. Bu hüquq inanclarına sərbəst riayət etmək azadlığını və hər hansı bir şəkildə və dövlət sərhədlərindən asılı olmayaraq informasiya axtarmaq, əldə etmək və yaymaq azadlığını özündə cəmləşdirir."

1966-cı ildə ABŞ-da "İnformasiya azadlığı haqqında" qanun, 1976-cı ildə isə "Açıq hökumət" haqqında qanun qəbul edildi. Bu qanunlar açıq informasiyaların mövcudluğu ilə bağlıdır. Çünki, informasiya ehtiyatlarının açıq informasiya ehtiyatı kimi formalaşması və onlardan istifadə problemi var. Oxşar aktlar Avropa Şurası və onun Nazirlər Komitəsi, habelə ayrı-ayrı Avropa ölkələri tərəfindən qəbul edilir.

Hal-hazırda dünyada açıq informasiyaların mövcudluğunu təmin etmək üçün qlobal informasiya şəbəkələrinin imkanlarından getdikcə daha çox istifadə olunur. Qərbdə ABŞ, Kanada və Böyük Britaniyadan, şərqdə Yaponiya, Malayziya və Filippinə qədər bir çox dövlət İnternetdə dövlət orqanlarının fəaliyyəti və vətəndaşlarla interaktiv əlaqə haqqında hərtərəfli məlumatın verilməsini nəzərdə tutan "elektron hökumətlər" in yaradıldığını elan etmişdir.

II istiqamət:

Gizlilik hüququnun qorunması. Bu ən uzun qanunverici tarixə sahib olan əsas konstitusiya hüquqlarından biridir. Təbii hüquqlar anlayışı əvvəlcə 1689-cu ildə İngiltərə Parlamenti tərəfindən, 100 il sonra isə ABŞ Konstitusiyasının Hüquqlar

Qanununda qəbul edildi. İnformasiya sahəsi üçün bu hüquq Ümumdünya İnsan Hüquqları Bəyannaməsinin 12-ci maddəsində öz əksini tapmışdır.

III istiqamət:

Məhdud şəxsi informasiya almaq hüququnun qorunması. 60-cı illərin sonunda emal olunmuş məlumatların ümumi miqdarından sosial, maliyyə və polis məqsədləri üçün emalı həyata keçirilmiş xüsusi şəxslər haqqında xüsusi bir kateqoriya ayrıldı. Bu informasiyalar ümumiləşdirilmiş "şəxsi məlumatlar" adını almışdır. Qərb ölkələrində kompüter elminin inkişafı və fərdi hüquqların pozulması təhlükəsinin artması (nəzarətsiz giriş və fərdi məlumatların yayılması), məlumatlandırma amilini nəzərə alan xüsusi aktların hazırlanmasını tələb etməyə başladı. Şəxsi məlumatların mühafizəsi ilə bağlı ilk qanunverici təşəbbüslər Almaniyada (Hesse) 1970-ci ildə dövlət idarəçiliyi və inzibati işlərin avtomatlaşdırılması üçün nəzərdə tutulmuş böyük kompüter mərkəzlərinin və ümumiləşdirilmiş məlumat bazasının yaradılmasına reaksiya olaraq ortaya çıxdı. Qanunvericilik təşəbbüslərinin müəllifləri haqlı olaraq hesab edirdi ki, informasiyanın mühafizəsi üçün tədbirlər görmədən onların avtomatik emal olunması vətəndaşların şəxsi azadlığına təhlükə yaradır və nəticədə vətəndaş cəmiyyəti üçün yeni təhlükə yaradır. Bu müəllilər informasiya axınlarının "ictimai həyatın sinir mərkəzini" meydana gətirdiyinə və vətəndaşlar haqqında məlumat sahibi olmağın "sosial qüvvə" olduğu ehtimalına əsaslanırdılar. 1970-ci ildə Hesse ərazisində İnformasiya Qoruma Komissarı ilk dəfə parlament tərəfindən seçilmiş və müstəqil bir "səlahiyyət" sahibi olmuşdur. Hökümətin qərarına görə, Müvəkkil avtomatlaşdırılmış bürokratiya qarşısında vətəndaşların çarəsizlik hisslərini aradan qaldıra biləcək bir "nümunə" olmalı idi. Belə ki, müvəkkil informasiyaların emalına birbaşa cavabdeh deyil, başqa heç bir orqan ona təlimat verə bilməz və onun nəzarətçi vəzifələri yoxdur.

Sonrakı 25 il İnformasiyanın Müdafiəsi üzrə Müvəkkil institutunun sadəcə qorunub saxlanılmadığını, həm də fərdin, cəmiyyətin və dövlətin maraqlarını tarazlaya biləcək təsirli bir mexanizmə çevrildiyini göstərdi. Bu müddət ərzində,

demək olar ki, bütün inkişaf etmiş Qərb ölkələrində bu sahə inkişaf etmişdir. Məsələn, bunun sayəsində 100 nəfərin iştirakı ilə Almaniyada şəxsi infomasiyanın təməl hüququ kimi mühafizəsi hüququnu qanuniləşdirmək və konstitusiya norması hesab etmək mümkünləşdi. Fərdin yeni əsas hüququ - informasiyanın öz müqəddəratını təyin etmə hüququ da formalaşdırılmış və qanuni şəkilə salınmışdır. Üstəlik, bu hüquq mütləq deyil, sosial inkişaf və dövlət idarəçiliyinin maraqlarına yönəlmiş bəzi məhdudiyyətlərə sahib olduğu da qəbul olunur.

Bir sıra ölkələrdə Müvəkkilin xidmətləri olduqca böyük bir əhəmiyyət daşıyır: bir ildə vətəndaşların pozuntularına və ya göstərilən hüquqların həyata keçirilməsinə dair 10-dan çox müraciətlərinə baxır, müraciət edənləri və s. qeyd edir. Belə ki, hər il Avropanın 12 ölkəsindən (14 il ərzində) çox sayda İnformasiya Qoruma Komissarları nümayəndələrinin illik toplantıları keçirilir və bu mühüm rol oynayır. Bu görüşlərdə yeni informasiya texnologiyalarının cəmiyyətə təsirindən yaranan yeni təhlükələrin təhlili aparılır.

70-ci illərin sonunda sonradan kompüter elmləri haqqında milli qanunvericilikdə əks olunan iki prinsip tərtib edilmişdir:

- kompüter sistemlərində məxfiliyin məhdudlaşdırılması;
- vətəndaşları bu cür müdaxilədən qorumaq üçün inzibati mexanizmlərin tətbiqi.

Bu istiqamətə Avropa Parlamentinin "Kompüter elminin tərəqqisi ilə əlaqədar şəxsi hüquqların qorunması haqqında" (1979) və Avropa Birliyinin "Fərdi məlumatların avtomatik işlənməsi ilə şəxslərin müdafiəsi haqqında" Konvensiyası (1980) daxildir.

IV istiqamət:

Fərdin əqli mülkiyyət hüquqlarının qorunması. Müəllif hüquqlarının qorunması üçün əsas beynəlxalq normalar 1967-ci ildə Stokholm Konfransı Konvensiyasına uyğun olaraq yaradılan Ümumdünya Əqli Mülkiyyət Təşkilatının hüquqi aktları ilə müəyyən edilir. Əqli mülkiyyət hüquqlarının qorunması uzun bir

beynəlxalq keçmişə malikdir. Dünyada əqli mülkiyyət qorunmasının inkişafına müxtəlif yanaşmalar mövcuddur.

Əvvəllər sənayeləşmiş ölkələr yaradıcılıq prosesinin tədqiqatı və inkişafı üçün həm özəl, həm də dövlət mənbələrini yaratdılar. Müəllif hüquqları ilə qorunan əsərlərin qiymətinin daimi artış sənayeləşmiş ölkələri əqli mülkiyyət hüquqlarının qorunması sistemini daha da təkmilləşdirməyə məcbur etdi. Tədricən qorunma kompüter proqramlarına və inteqral sxemlərə yayıldı və bu günə qədər bu ölkələr müəllif hüquqlarının ədalətsiz istifadəsinə qarşı durmaq üçün ciddi bir söz haqqına sahibdirlər.

İnkişaf etməkdə olan ölkələrdə əqli mülkiyyət hüquqlarının qorunması təkamülü fərqli bir formada baş verdi. Bəziləri köhnə müstəmləkə hakimiyyətlərindən miras qalan əqli mülkiyyət hüquqlarının qorunması səviyyəsini qorumaqla məhdudlaşdılar. Çox vaxt bu inkişaflarının ilk onilliklərində qanunvericiliklə bağlı idi. Digər ölkələrdə isə əqli mülkiyyət hüquqlarının qorunma səviyyəsi siyasi əqidəsinə uyğun olaraq, kapitalizmin istənməyən qalığı kimi göründüyünə və ya patent qorunması sürətli sənayeləşməyə maneə kimi göründüyünə görə azalmışdır. Bütün bunlar dünyanın müxtəlif ölkələrində qeyri-bərabər müdafiənin qurulmasına səbəb oldu və bəzi inkişaf etməkdə olan ölkələr və son sənayeləşmə dövrünün bəzi ölkələri əqli mülkiyyət hüquqlarının tamamilə qorunmasını təmin etmədi.

Müxtəlif ölkələrdə İT üzrə hüquqi tənzimləmələr fərqli ola bilər. Məsələn, qonşu ölkələrə nəzər salaq:

Türkiyədə “Elektron Rabitə Təhlükəsizliyi Tənzimlənməsi” adı altında müəyyən tədbirlər toplusu həyata keçirilir. Bu tənzimləmənin məqsədi elektron rabitə təhlükəsizliyi ilə bağlı prosedurları və prinsipləri nizamlamaqdır. Bu qayda fiziki məkan təhlükəsizliyini, informasiya təhlükəsizliyini, aparat-proqram təminatını və etibarlılığı və işçilərin etibarlılığını təmin etmək üçün təhdid və ya

zəif nöqtələrdən yaranan risklərin aradan qaldırılması və ya azaldılması ilə bağlı operatorların həyata keçirəcəyi tədbirləri və qaydalarını əhatə edir.

Bundan başqa, 2007-ci ildə 5651 saylı “internetdə nəşrlərin tənzimlənməsi və bu nəşrlər vasitəsi ilə törədilən cinayətlərə qarşı mübarizə haqqında” Qanun qüvvəyə minmişdir. Bu Qanunun məqsədi və əhatə dairəsi məzmun provayderinin, sayt təminatçısının, giriş təminatçısının və kollektiv istifadə təminatçılarının və internet mühitində məzmun, yer və giriş təminatçıları vasitəsilə törədilmiş müəyyən cinayətlərin öhdəlikləri və məsuliyyətləri ilə mübarizə prinsipləri və qaydalarını tənzimləməkdir.

5237 saylı Cəza Qanununun 1-ci bəndinə əsasən, qanunsuz bir şəkildə informasiya sisteminin hər hansı bir hissəsinə və ya bütününə daxil olan və orda qalan hər kəs 1 (bir) ilədək həbs cəzasına və ya məhkəmə cəzasına məhkum edilir.

2-ci bəndə əsasən, 1-ci bənddə göstərilən hərəkətlər müəyyən məbləğ qarşılığında istifadə oluna bilən sistemlərdə işlənildiyi təqdirdə veriləcək cəza yarı miqdarına qədər endirilir.

3-cü bənddə isə, sistemdəki məlumatların bu hərəkətə görə məhv edilib və ya dəyişdirilərsə, 6 (altı) aydan 2 (iki) ilə qədər həbs cəzasının tətbiq edildiyi qeyd olunub.

244-cü maddəyə əsasən, informasiya sisteminin fəaliyyətinə müdaxilə edən və ya fəaliyyətini pozan şəxs 1 (bir) ildən 5 (beş) ilə qədər azadlıqdan məhrum edilir. İnformasiya sistemindəki məlumatları məhv edən, dəyişdirən və ya əlçatmaz hala gətirən, məlumatları sistemə yerləşdirən və mövcud məlumatları başqa yerə göndərən şəxs 6 (altı) aydan 3 (üç) ilə qədər həbs cəzasına məhkum edilir. Bu əməllər bir bankın və ya kredit təşkilatının və ya bir dövlət qurumunun və ya təşkilatın informasiya sistemində edilərsə, cəza yarı qədər artırılır.

Digər qonşu ölkə olan Rusiyada 20 fevral 1995-ci il tarixli, 24-FZ nömrəli "İnformasiya, informasiyalaşdırma və informasiyanın qorunması haqqında" qanun informasiya təhlükəsizliyi haqqında Rusiya qanunları arasında əsas sayılan

qanundur. Qanun məlumatların məxfiliyinin qorunmasının ən üst səviyyədə təşkili üçün bütün növ tədbirlər kompleksi ilə təchiz olunmuşdur. Bundan başqa, "İnformasiya, İnformasiya texnologiyaları və Məlumat qoruması haqqında" 27 iyul 2006-cı il tarixli 149-FZ Qanunu da təhlükəsizliyin təmini üçün xüsusi əhəmiyyətə malikdir.

Dövlət maraqlarının qorunması problemi bu sahədə milli prioritetləri müəyyən edən kifayət qədər inkişaf etmiş milli qanunvericiliyin köməyi ilə həll olunur. Avropa Birliyinə üzv dövlətlərinin inteqrasiyası bu sahədə əlaqələndirməni tələb edir. Bunun nəticəsində gizli məlumatların ümumi prinsipləri Məxfiliyin Mühafizəsi Konvensiyasında öz əksini tapdı. Müdafiə mexanizmi aşağıdakı aspektləri əhatə edir:

• qorunmanın prioritetliyi;

• müdafiə mexanizmlərinin, icra mexanizmlərinin və tənzimləmə dəstəyinin müəyyən edilməsi.

Belə nəticəyə gəlmək olar ki, müxtəlif ölkələrin dövlət sirri təşkil edən məlumatlarının mühafizəsi problemi yalnız dünya birliyinin digər üzvlərinin təhlükəsizliyi təmin edildiyi təqdirdə həll edilməlidir. Məsələn, beynəlxalq hüquq normaları digər dövlətlərin ekoloji təhlükəsizliyinin asılı olduğu gizli məlumatların ələ keçməsinin qarşısını alır.

Dünya praktikasında dövlət sirrlərinin sayının azalması və dövlət orqanlarının fəaliyyətinin "şəffaflığının" artması tendensiyası getdikcə daha çox nəzərə çarpır. Klinton rəhbərliyi dövründə (1991-2000) ABŞ dövlət qurumlarının açıqlanmayan rəsmi sənədlərinin sayına görə bir növ rekorda imza atdı. Arxivlərin gizlədilməsinin təşəbbüskarı olan konqresmen David Skegs öz çıxışında bunu "dövlət sirlərini qorumağın həqiqi dəyərini açıqlamaq bizə arxiv sistemini islah etməyə və amerikalıların vergi yükünü azaltmağa imkan verəcəkdir" ifadələriylə bəyan etmişdir.

Beləliklə, 1999-cu ildə ABŞ-da 127 milyon səhifəlik məxfi sənəd, proqram müddətində isə, yəni, 1995-1999-cu illərdə isə 789 milyon səhifə açıqlandı. Müqayisə üçün qeyd edək ki, 1980-1994-cü illərdə bu rəqəm 188 milyon səhifə idi. Məxfilik möhürünü itirən sənədlər İnternet vasitəsi ilə onlara pulsuz daxil olmaq üçün Konqres, Prezident Administrasiyası, CİA, Pentaqon və digər şöbələrin elektron kataloqlarına yerləşdirilib.

Biznes və maliyyə fəaliyyətinin qorunması. Bu "ticarət sirri" anlayışını müəyyən edən, "ədalətli" rəqabətin həyata keçirilməsi üçün şərait yaradan və sənaye casusluğunu haqsız rəqabətin elementi kimi qiymətləndirən qanunverici bir mexanizm yaratmaqla həll olunur. Bu istiqamətə aşağıdakılar daxil ola bilər:

- inhisarçılığın qarşısını alan qanunların tətbiqi;
- ədalətli rəqabət mexanizmlərinin yaradılması;
- proqram məhsulları müəlliflərinin hüquqlarının qorunması mexanizmlərinin tətbiqi.

Sonuncu istiqamət AB-nin "Kompüter proqramları və məlumat bazalarının qorunması haqqında" (1990) direktivində əks olunur. Kommersiya məlumatlarının qorunması üçün beynəlxalq səviyyədə hazırlanmış konseptual çərçivə və prinsiplər Böyük Britaniya, Fransa, Almaniya, ABŞ, Kanada və digər ölkələrin milli qanunlarında öz əksini tapmışdır. Bu sahədə ən inkişaf etmiş qanunvericilik yüzdən çox fərqli aktın qüvvədə olduğu ABŞ-dadır və ilk qanunlar XX əsrin əvvəllərində hazırlanmışdır [7].

Qərbdə məlumatların emalı və ötürülməsi vasitələrinin inkişafı bu sahədə cinayətlərin artmasını da özü ilə bərabər gətirmişdir. Bu tip cinayətkarlıq qüvvələrinin sayının sürətlə artması ölkələri cəzaların sərtləşdirilməsi istiqamətində milli qanunvericiliyi təkmilləşdirməyə sövq etmişdir.

ABŞ-ın informasiyalaşdırma və informasiya təhlükəsizliyi haqqında qanunu aşağıdakıları təmin edir:

- informasiyalaşdırma sahəsində dövlət siyasətinin müəyyənləşdirilməsi;

- inkişaf etmiş istehsal və texnologiyaları təmin etmək;
- inhisarçılığa qarşı mübarizə və prioritet sahələrin stimullaşdırılması;
- informasiya sistemlərinin təşkili;
- bu sahədə idarəetmə sistemlərinin yaradılması;
- istehlakçı hüquqlarının, xüsusən vətəndaşların informasiya hüquqlarının qorunması, vətəndaşlar haqqında informasiyaların qorunması;
- kompüter proqramı istehsalçılarının hüquqlarının tənzimlənməsi.

Müxtəlif ölkələrin qanunlarında göstərilən məlumatlardan sui-istifadə üçün məsuliyyət bütün bu ölkələr üçün ümumi məqamlar ilə xarakterizə olunur:

- bütün inkişaf etmiş ölkələrdə fərdi məlumatların işlənməsi və istifadəsinin pozulmasına görə məsuliyyət müəyyən edilmişdir;
- informasiya (kompüter) cinayətləri vətəndaşlar, cəmiyyət, dövlət üçün xüsusi təhlükə yaradan və kompüter texnikasından istifadə edilmədən törədilmiş oxşar cinayətlərə nisbətən daha ağır cəzalara səbəb olan cinayətlər kimi qəbul edilir;
- cinayətlər də zərər təhdidi yaradan hərəkətlər hesab olunur, məsələn sistemə daxil olmaq cəhdi, kompüter viruslarının tətbiqi və s.

İnformasiya təhlükəsizliyinin təmin edilməsi üçün hüquqi bazanın inkişafındakı mövcud tendensiyaların təhlili, dünya birliyinin özəl məlumatları qorumaq hüquqlarının pozulmasının yolverilməzliyi barədə dünya ictimaiyyətinin sarsılmaz görünən mövqeyini dəyişdirdiyinə dair nəticəyə gəlməyə imkan verir. Buna səbəb məhz son zamanlarda beynəlxalq terrorizm tərəfindən kəskin artan təhdidlər oldu.

11 sentyabr 2001-ci ildə Nyu-Yorkda və 24-26 oktyabr 2002-ci ildə Moskvada baş verən hadisələr hökuməti telefon danışığı zamanı, elektron poçt və fakslar vasitəsi ilə ötürülən informasiyaya dövlət nəzarətinin zəruriliyinə yenidən nəzər salmağa məcbur etdi.

Bununla əlaqədar, 30 may 2002-ci ildə Avropa Parlamenti elektron şəkildə ötürülən məlumatların mühafizəsi ilə bağlı kompromis qanun layihəsinin lehinə səs verdi. Radikal versiyada Avropa hökumətlərinin elektron rabitə üzərində daha çox nəzarət etmək istəyi əks olunurdu, kompromis isə insan hüquqlarının qorunmasını vurğuladı. Güzəşt odur ki, AB dövlətləri araşdırma məqsədləri üçün elektron poçtların, İnternetin və telefon rabitəsinin monitorinqi tələb olunduğu hallarda vətəndaşların şəxsi sirləri üzərindəki hüquqlarına maksimum riayət edilməsi tövsiyə olunur. Eyni zamanda, qanunda belə monitorinqə icazə verən və ya qadağan edən məcburi müddəalar yoxdur. Hər bir ölkə öz qaydalarını özü müəyyənləşdirəcəkdir.

Qanun layihəsinin digər müddəaları arasında, elektron poçt qutuları və ya mobil telefonlar vasitəsi ilə reklamların şəxsi istifadəçilərə onların razılığı olmadan göndərilməsi, ayrı-ayrı abunəçilərin telefon nömrələrinin, elektron poçt ünvanlarının ictimai qovluqlarda yayımlanmaması hüququ və s. yer alır.

Dünyada informasiya təhlükəsizliyinin təmin edilməsinin digər vacib bir sahəsi elektron sənədlərin və elektron ticarətin qorunmasıdır. Bu qanunvericilik sahəsində əsas vəzifələrə digər media növləri ilə birlikdə elektron informasiya formalarının bərabər istifadəsi üçün hüquqi bazanın genişləndirilməsi və informasiya məhsulları və texnologiyalarının yaradılması, yayılması və istifadəsi ilə bağlı məhdudiyyət və maneələrin sayının azaldılması daxildir. Hal-hazırda, bir çox ölkədə elektron ticarət və elektron sənədlər haqqında qanunların qüvvəyə minməsi üçün işlər görülür. Bu, təkcə ABŞ kimi informasiya nəhənginə çevrilmiş ölkələrə aid deyil. Oxşar qanunlar Belarus Respublikasında və hətta Türkmənistanda da qəbul edilmişdir.

2.3. İnformasiya təhlükəsizliyinin hüquqi təminatı sahəsində dövlət siyasətinin əsasları

Qısaca tarixi məlumat verək. İT sahəsində qanunvericilik bazasının formalaşmasında dünya meyllərinə uyğun olaraq, ilk aktlar Rusiyada dövlət sirlərinin qorunması üçün hazırlanmışdır. İlk dəfə hərbi casusluq məsuliyyəti dövlətə xəyanət forması kimi Cinayət və İslah hökmləri məcəlləsində və 20 aprel 1892-ci il tarixli qanunla Cinayət İşləri Nizamnaməsində tətbiq edilmişdir. 1912-ci ildə isə sülh dövründə casusluq yolu ilə dövlətə xəyanət haqqında qanunların dəyişdirilməsinə dair ayrıca Qanun qəbul edildi. Hərbi sahə ilə bağlı dövlət sirrinin yeni tərifi təqdim edildi. Bu qanuna görə, dövlət sirri "Rusiyanın və ya ölkənin silahlı qüvvələrinin və strukturlarının xarici təhlükəsizliyi ilə əlaqəli informasiya və ya obyektlər" kimi başa düşülürdü.

Birinci Dünya Müharibəsi başlayandan sonra bu problemə diqqət daha da gücləndi. Belə ki, 20 iyul 1914-cü ildə "Hərbi senzura haqqında Müvəqqəti Nizamnamənin təsdiq edilməsi haqqında" fərman qüvvəyə mindi və ilk dəfə hərbi sirr təşkil edən məlumatların da siyahısı tərtib edildi. Bu siyahıdakı ən gizli məlumatlar isə "gizli saxlanılmalıdır" başlığı altına düşdü.

XX əsrin əvvəllərində Rusiya qanunvericiliyində casusluq "xarici dövlətə Rusiyanın xarici təhlükəsizliyi ilə əlaqəli məlumat və ya əşyaların toplanmasına və ölkəni qorumaq üçün nəzərdə tutulmuş silahlı qüvvələrə və ya quruluşlara kömək etmək" demək idi. Gizli məlumatların xarici bir dövlətin maraqları üçün yayılması və ya yayımlanması 1912-ci il Qanununa görə 15 ilədək ağır əmək cəzası tətbiq olunmaqla yüksək xəyanətin ən ağır forması hesab olunurdu [8].

İnformasiyalaşdırma sahəsində qanunvericiliyin inkişaf etdirilməsinin zəruriliyi məsələsi nəzəri cəhətdən 60-cı illərdə SSRİ Elmlər Akademiyasının Dövlət və Hüquq İnstitutunun mütəxəssisləri tərəfindən qaldırılmışdı. Ancaq bu məsələyə praktikada əsasən Ryad seriyalı böyük kompüterlərin istifadəsinə istiqamətlənmiş müxtəlif səviyyəli avtomatlaşdırılmış idarəetmə sistemlərinin inkişafı ilə əlaqədar olaraq yalnız 70-ci illərdə baxılmağa başlandı. Qanuni dəstək termini ilə ifadə olunan normativ baza, quruluş və həyata keçirilmə mexanizmləri,

şöbə aktlarından, SSRİ hökumətinin bir neçə qərarından və respublika səviyyəli analoji aktlardan kənara çıxmadı.

Təəssüf ki, 70-ci illərin sonlarında görülən Avropa Birliyi Şurasının işi demək olar ki, diqqətdən kənarda qaldı. Kompüterlə işlənən fərdi informasiyaların qorunması, ticarət sirlərinin qorunması haqqında qanun və sonradan bir sıra Avropa ölkələrinin milli qanunvericiliyində əks olunmuş bəzi digər tövsiyələrə aiddir. Qanunvericilik problemi Rusiya Sovet Federativ Sosialist Republikası - RSFSR Cinayət Məcəlləsinin üç maddəsi və SSRİ hökuməti tərəfindən təsdiq edilmiş bir sıra normativ aktlarla həyata keçirildi.

İnformasiya təhlükəsizliyini, cəmiyyətin kriminallaşmasını, Rusiyada getdikcə inkişaf edən kompüter vasitələrindən istifadə etməklə törədilən cinayətlərin yüksək məxfiliyini təmin edən informasiya texnologiyalarının geriliyi, bu cür cinayətlərin sübutunun mürəkkəbliyi Rusiyada informasiya cinayətlərinin inkişafı üçün son dərəcə əlverişli şərait yaratdı. 1991-1992-ci illərdə ölkədə informasiya mühitində bir sıra bu səpkidə cinayətlər törədildi, dəyən ümumi zərər isə on minlərlə milyard rubl təşkil etdi. Bu cür cinayətlərin davamlı olaraq artmasına yönəlmiş tendensiya hələ də davam edir. Avqustun sonunda Moskvada 125.500 dollar oğurlayan cinayətkar qrupun fəaliyyəti dayandırıldı.

Rusiya Federasiyasında İT ilə bağlı qanunvericiliyin formalaşdırılmasına nəzər salaq. İnformasiya təhlükəsizliyini təmin etmək sahəsində qanunvericilik işinin məqsədi planların spekulyativ quruluşundan, parçalanmış qanunvericilik dizaynından və köhnəlmiş şöbə və yerli aktlardan bu məsələ ilə bağlı xüsusi qanunvericiliyin sistemli şəkildə formalaşdırılmasına və həyata keçirilməsinə keçmək idi. Bu yanaşmada tələb olunur:

- hərtərəfli təşkilati və qanun layihəsi hazırlanması;
- bu sahədə hüquqi şüurun formalaşdırılması üzərində sistemli iş;
- qəbul edilmiş qanunların və digər tənzimləyicilərin tətbiqi və icrasını təmin edən mexanizmlərin yaradılması.

1990-1992-ci illərdə Rusiya Dövlət Texniki Komissiyasının bəyan edilmiş mövqeyini nəzərə alaraq, Obninsk və Sankt-Peterburq şəhərlərində İnformasiya Təhlükəsizliyi probleminin hüquqi dəstəklənməsi məsələlərinin müzakirə olunduğu iki konfrans keçirildi. Dövlət Texniki Komissiyasının mütəxəssisləri bir sıra daxili və beynəlxalq konfransların təşkili və keçirilməsində iştirak etdilər. Bunlardan "Aerokosmik kompleksin konversiyası" (sentyabr 1992), "Biznes və təhlükəsizlik" (oktyabr 1992) kofranslarının adını çəkmək olar. İlk dəfə Rusiya Dövlət Texniki Komissiyasının nümayəndəsi Avropa Birliyinin informasiya təhlükəsizliyi üzrə işçi qrupunun işində iştirak etdi (sentyabr 1992, Berlin).

Tarixi faktlar əsasında Rusiya Federasiyasının (RF) informasiya təhlükəsizliyi sahəsində kifayət qədər yenilikçi addımlar atdığını görürük. Bu səbəblə, RF-nin beynəlxalq informasiya təhlükəsizliyi sahəsində 2020-ci ilə qədər olan dövlət siyasətinin əsaslarına nəzər salaq. RF-nin dövlət siyasətinin məqsədi beynəlxalq informasiya təhlükəsizliyi sisteminin formalaşması üçün şərait yaratmağa yönəlmiş beynəlxalq hüquqi rejimin qurulmasına kömək etməkdir. Rusiya Federasiyasının ikitərəfli, çoxtərəfli, regional və qlobal səviyyədə beynəlxalq informasiya təhlükəsizliyi sisteminin yaradılması probleminin həlli ilə bağlı dövlət siyasətinin əsas istiqamətləri bunlardır:

- Birləşmiş Millətlər Təşkilatına üzv dövlətlər tərəfindən beynəlxalq informasiya təhlükəsizliyi haqqında Konvensiyanın hazırlanması və qəbul edilməsi zərurətində Rusiya təşəbbüsünün beynəlxalq aləmdə təbliği üçün şərait yaradılması.
- Birləşmiş Millətlər Hökuməti Ekspertlər Qrupunun beynəlxalq təhlükəsizlik kontekstində məlumatlandırma və telekommunikasiya sahəsindəki nailiyyətləri ilə əlaqədar işlərinin nəticəsi olaraq verilmiş yekun sənədlərdə beynəlxalq informasiya təhlükəsizliyi sisteminin qurulması sahəsində Rusiya təşəbbüslərinin birləşdirilməsini təşviq etmək,
- “İnternet” informasiya və telekommunikasiya şəbəkəsinin idarəçiliyinin

beynəlxalq miqyasda təşəbbüsü və bu kontekstdə Beynəlxalq Telekommunikasiya İttifaqının rolunun artırılması istiqamətində Rusiya təşəbbüsünün beynəlxalq aləmdə təbliği;

Dövlət siyasəti 8 əsas müddəadan ibarətdir.

1. Bu əsaslar Rusiya Federasiyasının strateji planlaşdırma sənədidir.

2. Bu əsaslar beynəlxalq informasiya təhlükəsizliyi sahəsindəki əsas təhdidləri, Rusiya Federasiyasının beynəlxalq informasiya təhlükəsizliyi sahəsində dövlət siyasətinin məqsədini, məqsədlərini və prioritet sahələrini (bundan sonra - Rusiya Federasiyasının dövlət siyasəti), habelə onların həyata keçirilmə mexanizmlərini müəyyənləşdirir.

3. Bu Prinsiplərin tənzimləyici hüquqi bazası RF-nin Konstitusiyası, RF-nin beynəlxalq informasiya təhlükəsizliyi sahəsindəki beynəlxalq müqavilələri, federal qanunları, RF-nin Prezidentinin və RF hökumətinin normativ hüquqi aktları, RF-nin digər normativ hüquqi aktları ilə qurulur.

4. Bu Prinsiplərdə RF-nin 2020-ci ilədək Milli Təhlükəsizlik Strategiyasının, RF-nin İnformasiya Təhlükəsizliyi Doktrinası, Xarici Siyasət Konsepsiyası və digər strateji planlaşdırma sənədlərinin konkret müddəaları göstərilir.

5. Bu əsaslar nəzərdə tutulub:

a) beynəlxalq informasiya təhlükəsizliyi sisteminin formalaşdırılması, o cümlədən hüquqi, təşkilati və digər dəstək növlərinin təkmilləşdirilməsi sahəsində Rusiya təşəbbüslərini beynəlxalq aləmdə təbliğ etmək;

b) Rusiya Federasiyasının beynəlxalq informasiya təhlükəsizliyi sahəsində dövlət siyasətinin həyata keçirilməsində idarələrarası əməkdaşlığı təşkili etmək;

c) iqtisadiyyatın real sektorunda informasiya və kommunikasiya texnologiyalarının daha geniş istifadəsi səbəbindən aparıcı dünya gücləri ilə texnoloji paritetə nail olmaq və saxlamaq.

6. Beynəlxalq informasiya təhlükəsizliyi dedikdə, qlobal informasiya məkanında bir şəxsin, cəmiyyətin və dövlətin informasiya sahəsindəki hüquqlarının pozulması, habelə milli kritik informasiya infrastrukturunun elementlərinə dağıdıcı və qanunsuz təsirlərin istisna olunduğu bir vəziyyət başa düşülür.

7. Beynəlxalq informasiya təhlükəsizliyi sistemi qlobal informasiya məkanının müxtəlif subyektlərinin fəaliyyətini tənzimləmək üçün hazırlanmış beynəlxalq və milli qurumların məcmusunu ifadə edir. Beynəlxalq informasiya təhlükəsizliyi sistemi strateji sabitliyə təhdidlərə qarşı çıxmaq və qlobal informasiya məkanında ədalətli strateji tərəfdaşlığı təşviq etmək üçün hazırlanmışdır. Beynəlxalq informasiya təhlükəsizliyi sisteminin yaradılması sahəsində əməkdaşlıq Rusiya Federasiyasının milli maraqlarına cavab verir və onun milli təhlükəsizliyinin möhkəmləndirilməsinə kömək edir.

8. Beynəlxalq informasiya təhlükəsizliyi sahəsində əsas təhlükə informasiya və kommunikasiya texnologiyalarının istifadəsidir:

a) beynəlxalq hüquq normalarına zidd olan hərbi-siyasi məqsədlər üçün, suverenliyi ləkələməyə, dövlətlərin ərazi bütövlüyünü pozan və beynəlxalq sülhə, təhlükəsizliyə və strateji sabitliyə təhlükə yaradan düşmənçilik hərəkətləri və təcavüz aktları həyata keçirmək üçün informasiya silahı olaraq;

b) terror məqsədləri üçün, o cümlədən kritik informasiya infrastrukturunun elementlərinə dağıdıcı təsir göstərmək, terrorizmi təşviq etmək və terrorçu fəaliyyətə yeni tərəfdarları cəlb etmək üçün;

c) suveren dövlətlərin daxili işlərinə qarışdığına, ictimai qaydanı pozduğuna, millətlərarası və dinlərarası düşmənçiliyə təhrik etdiyinə, nifrət və ayrıseçkilik

yaradan, zorakılığa təhrik edən irqçi və ksenofobik fikir və ya nəzəriyyələri təbliğ etdiyinə görə;

d) istifadəsi və yayılması ilə kompüter məlumatlarına qeyri-qanuni giriş ilə əlaqəli olan cinayətlər də daxil olmaqla, zərərli kompüter proqramlarının yaradılması üçün.

İnformasiya uğurlu təşkilatlar üçün vacib bir vasitədir və İnformasiya Təhlükəsizliyi Qanunu bu tənliyin əsas hissəsini təşkil edir. İnformasiya Təhlükəsizliyi Qanunu bu məlumatı və onu emal edən informasiya sistemlərini icazəsiz girişdən qorumağı tələb edən qanun normaları, kodlar və standartların məcmusudur.

Təhlükəsizliyin təmin edilməsi dəyərin təmin olunması ilə bağlıdır. Nağd pul, qızıl və ya zinət əşyaları kimi fiziki dəyərlərimizi oğurluq, itki və ya məhv olmaya qarşı qoruduğumuz kimi, eynilə də bu diqqəti rəqəmsal dəyərlərə - xüsusən də, informasiyaya göstərməliyik. Çünki, biz informasiya cəmiyyətində yaşayırıq və məlumatın yaradılması, istifadəsi və yayılması mühüm iqtisadi, siyasi və mədəni fəaliyyət kimi qiymətləndirilir. Və artıq bu dövrdə xidmət iqtisadiyyatından kompüter, mobil qurğular və internet kimi informasiya texnologiyalarına güvənən fəaliyyətləri vurğulayan informasiya iqtisadiyyatına keçirik.

İnformasiya təhlükəsizliyinin təmini üçün qanunlar vacibdir, çünki informasiyanın müəyyən dəyəri var.

Bu ssenaridə aşağıdakı addımlar atılır:

- Riskləri müəyyənləşdirmək - informasiya üçün bütün riskləri müəyyənləşdirilir.
- Qoruyucu tədbirləri müəyyənləşdirmək - risklərə əsaslanan fiziki, rəqəmsal, əməliyyat və inzibati təminatları müəyyənləşdirmək.
- Təhlükəsizlik tədbirləri yaratmaq - risklərə qarşı təhlükəsizlik tədbirləri yaratmaq.

- Təhlükəsizlik tədbirlərini yoxlamaq - mühafizə tədbirlərinin işlədiyini yoxlanılır.
- Təhlükəsizlik tədbirlərini yeniləmək - hər hansı bir yeni risk üçün bu təminatları yenilənməlidir.

1992-ci ilin aprelində təsdiq edilən "İnformasiyalaşdırma sahəsində iş üçün qanunvericilik və tənzimləmə dəstəyinin hazırlanması" Proqramına uyğun olaraq, informasiyalaşdırma və informasiya təhlükəsizliyi sahəsində aşağıdakı qanunvericilik aktları qəbul edilməli idi:

- "İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında",
- "İnformasiyadan sui-istifadə hallarına görə məsuliyyət haqqında",
- "beynəlxalq informasiya mübadiləsində iştirak və informasiya məhsullarının ixracına nəzarət haqqında",
- "MDB üzvü olan dövlətlərin məlumatlandırma sahəsində əməkdaşlıq haqqında Sazişi"
- "Dövlət sirri haqqında"
- "Kommersiya sirləri haqqında" proqram

Proqramın həyata keçirilməsi zamanı isə müəyyən mərhələlər həyata keçirilməli idi:

• Rusiyada informasiyalaşdırma və informasiyaların qorunması prosesi üçün hüquqi bazanın yaradılması;

• vətəndaşların, təşkilatların və dövlətin informasiya əldə etmək hüququnun normativ cəmləşdirilməsi;

• dövlət və kommersiya sirrinin qorunması qaydalarını, informasiyanın və bütövlükdə informasiya ehtiyatının hüquqi, təşkilati və texniki qorunması qaydalarını, qorunma əsaslarını və istehlakçı hüquqlarının qanuni təminatlarını

nəzərə alaraq informasiya və informasiya sistemlərinin hüquqi rejiminin yaradılması;

• informasiya və proqram məhsullarının müəllifinin və sahibinin hüquqlarının qorunması;

• Rusiyanın beynəlxalq informasiya mübadiləsində iştirakının qanuni qeydiyyatı, vahid hüquqi dəstək konsepsiyasında nəzərdə tutulmuş bir çox digər informasiyalaşdırma prosesinin hüquqi həlli.

Ancaq bu günə qədər informasiya təhlükəsizliyinin hüquqi təminatında kifayət qədər problemlər hələ də var. Bu sahənin hazırkı vəziyyəti və informasiya təhlükəsizliyinin hüquqi təminatı sahəsində dövlət siyasətinin əsasları 2000-ci ilin sentyabrında qəbul edilmiş İnformasiya Təhlükəsizliyi Doktrinasında təsvir edilmişdir.

İnformasiya təhlükəsizliyinin təmin edilməsi üçün hüquqi bazanın təkmilləşdirilməsi istiqamətində atılan mühüm addımlara baxmayaraq, bir sıra həll olunmamış problemlər hələ də qalmaqdadır. İnformasiya təhlükəsizliyi sahəsində hüquqi tənzimləmə praktikasının təhlili bizə deməyə imkan verir ki, hüquqi bazanın formalaşdırılması hüquq tətbiqetmə praktikasını düzgün təhlil etmədən və Rusiyanın üzvü olduğu beynəlxalq təşkilatların tövsiyələrini nəzərə almadan kifayət qədər qarışıq və sistemsiz vəziyyətdədir. Ekspertlərin fikrincə, informasiya sahəsində ictimai münasibətlərin hüquqi tənzimlənməsinin uyğunsuzluğu və inkişaf etməməsi ciddi mənfi nəticələrə səbəb olur:

- Fərdin şəxsi və ailə sirrinə olan konstitusiya hüquqlarının səmərəli həyata keçirilməsi və qorunması, şərəf və ləyaqətinin qorunması (bu, şəxsi məlumatları özündə saxlayan verilənlər bazalarının nəzarətsiz paylanması, bu cür məlumatların İnternetdə yayılması və s. ilə ifadə olunur);
- KİV azadlığına konstitusiya məhdudiyyətlərinin qoyulması konstitusiya quruluşunun əsaslarının, mənəviyyatının, sağlamlığının, vətəndaşların

hüquq və qanuni mənafelərinin qorunması, ölkənin müdafiə qabiliyyətinin və dövlət təhlükəsizliyinin təmin edilməsi baxımından zəif həyata keçirilir.

- Başlanğıcda icra hakimiyyəti orqanlarının saytlarının yaradılması ilə təmin olunmasına baxmayaraq, dövlət orqanları və yerli özünüidarəetmə orqanlarının şəxsin hüquq və azadlıqlarına birbaşa təsir edən məlumatlara sərbəst və tez bir zamanda daxil olması üçün əlverişli şərait yaradılmamışdır.
- Hüquq-mühafizə praktikası yeni informasiya texnologiyaları və kompüter şəbəkələrinin istifadəsi nəticəsində yaranan müasir təhdidlərə kifayət qədər cavab verə bilməyən dövlət sirlərini qoruma sistemlərinin qüsurlarını aşkar etmişdir;
- Elektron ticarətdə iştirak edənlərin hüquqlarının müdafiəsi təmin edilmir. Onlar daim təhlükə və risk altında işləyirlər. Bu risk alıcılar üçün xüsusilə böyükdür;
- Bir tərəfdən özünü göstərən informasiyaların düzgünlüyünü asanlıqla yoxlaya bilməməsində, digər tərəfdən, xüsusən seçki kampaniyaları çərçivəsində informasiyaların manipulyasiya vasitələri və metodlarının yayılmasında özünü göstərən informasiyaların manipulyasiyasına qarşı heç bir hüquqi mexanizm yoxdur;
- İnternetin inkişafı, İnternetdə əqli mülkiyyətdən istifadəyə nəzarətin mürəkkəbliyi və fəaliyyəti tənzimlənməyən elektron kitabxanaların paylanması ilə əlaqəli intellektual mülkiyyət hüquqlarının pozulma dərəcəsi artmışdır;
- Dövlət informasiya ehtiyatlarından istifadədə dövlətin və cəmiyyətin maraqlarının müdafiəsi yoxdur. İnformasiya ehtiyatlarının dövlət və milli aktivlər kimi təsnif edilməsi prinsipləri müəyyənləşdirilməyib, dövlət mənbələrinə maneəsiz giriş və onların yaradılması, inkişafı və saxlanılması qaydası təmin edilmir [9].

III FƏSİL. İNFORMASİYA TƏHLÜKƏSİZLİYİNİN HÜQUQİ TƏNZİMLƏNMƏSİNİN AZƏRBAYCANDA TƏTBİQİ

3.1. Azərbaycanda informasiya təhlükəsizliyi problemi

Son onillik Azərbaycanda cinayətkarlığın strukturunda kəskin dəyişikliklərlə, o cümlədən, onun böyüməsi, yeni cinayət növlərinin, onların törədilmə metodlarının qəbuluyla Azərbaycan Respublikasının yeni Cinayət Məcəlləsinin

meydana çıxması ilə səciyyələnir. Bunların arasında kompüter informasiyaları sahəsində cinayətlər də öz əksini tapır. Kompüter texnologiyası sahəsində qanunsuz hərəkətlərə qarşı mübarizə çox vaxt elmi-texnoloji tərəqqinin sürətli inkişafı ilə əlaqədar olur. Qlobal kompüterləşmə müasir cəmiyyətin, insanların, müəssisə və təşkilatların, dövlətin fəaliyyətinin demək olar ki, bütün aspektlərinə təsir göstərərək ictimai münasibətlərin yeni bir sahəsini meydana çıxartmışdır. Lakin təəssüf ki, onlar da çox vaxt qanunsuz hərəkətlərin obyektinə çevrilirlər.

Bununla birlikdə, hüquq-mühafizə orqanları cəmiyyətin və dövlətin hüquq və mənafelərini qorumaq üçün əhəmiyyətli maneələrlə rastlaşmış olur. Belə ki, kompüter informasiyaları sahəsində cinayətlər daim yenilənir və spesifik cinayət növləri formalaşır, cinayət hücumlarının müxtəlif obyektləri və metodları zaman keçdikcə daha tez gizlədiləbilmə xüsusiyyətinə malik olur. Bu da öz növbəsində, öncədən də qeyd etdiyim kimi, böyük maneə rolunu oynayır. Cinayətlərin ifşası və istintaqı sahəsində fəaliyyətlərin ümumi azalması ilə də vəziyyət biraz daha ağırlaşmış olur. Məsələn, hüquq-mühafizə orqanları cinayətkarlıqla mübarizə üçün yeni şərtlərə çox yavaş uyğunlaşır. Bu sürət maneələrin inkişaf sürəti ilə heç cür "tarazlıqda" ola bilmir.

Kompüter informasiyaları sahəsində cinayətlərin araşdırılması problemlərinin öyrənilməsi müasir məhkəmə-ekspertiza elminin ən aktual vəzifələrindən biridir. Son illərdə məhkəmə ədəbiyyatında kompüter cinayətlərinin araşdırılması texnikasına diqqət artırılmasına baxmayaraq, bu sahədə bir sıra həll olunmamış və mübahisəli məsələlər hələ də qalmaqdadır. Cinayətlərin kateqoriyası ilə bağlı orijinal dövlət statistikasının olmaması səbəbindən bu sahədəki nəticələr yalnız müəyyən sorğulara, anketlərə və aşağıdakı əsas istiqamətlərə əsaslanaraq əldə olunur.

- kompüter cinayətlərinin cinayət hüquqi xarakteristikası problemlərini təhlil etmək;
- kompüter cinayətlərinin kriminalist xarakteristikasının əsas elementlərini araşdırmaq;

- kompüter texnologiyalarından istifadə sahəsindəki cinayətlərlə əlaqəli işlər üzrə müfəttişin axtarış işlərinin obyektlərini öyrənmək;
- kompüter texnologiyalarından istifadə sahəsində cinayətlərin araşdırılmasının taktiki-təşkilati əsaslarını müəyyənləşdirmək;
- kompüter cinayətləri törətmiş şəxslərin müəyyənləşdirilməsi və axtarışı üçün tövsiyələr hazırlamaq.

Bütün bu nəticələri ümumiləşdirən hüquqi bazanın formalaşması da müəyyən dərəcədə kompüter informasiyası cinayətlərinin tədqiqi və bu fonda tədbirlər üçün önəmli nüans sayıla bilər.

Ölkəmizdə müstəqillik əldə olunduğu gündən bu sahədə hüquqi tənzimləmələr daim diqqət mərkəzində olmuş və zaman keçdikcə təkmilləşdirilmişdir. Azərbaycan Respublikasının informasiya qanunvericiliyinə bir sıra əsas qanunlar daxildir:

- "Kütləvi İnformasiya Vasitələri haqqında" Qanun,
- "İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında" Qanun və s.
- "İnformasiya əldə etmək haqqında" Qanun
- "Elektron imza və elektron sənəd haqqında" Qanun
- "Fərdi məlumatlar haqqında" Qanun
- "Elektron ticarət haqqında" Qanun və s.

Bu qanunvericilik aktları kompüter informasiyaları sahəsində əsas termin və anlayışları müəyyənləşdirmiş, onun yayılması, müəllif hüquqlarının qorunması, proqram təminatının və yeni informasiya texnologiyalarının yaradılması, həmçinin, onun hüquqi qorunması və istifadəsi ilə əlaqədar yaranan əmlak və qeyri-əmlak münasibətlərini tənzimləmişdir. İnformasiya təhlükəsizliyi və beynəlxalq informasiya mübadiləsi anlayışlarının qanunvericilikdə açıqlanması da həyata keçirilmişdir.

İnformasiya mühafizəsi fəaliyyətinin hüquqi təminatında ən mühüm addımlardan biri 1998-ci il 3 aprel tarixində “İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında” Qanunun qəbul edilməsi idi. Bu qanun texniki qurğularda və informasiya-telekommunikasiya xətlərində emal, saxlama və dövriyyə zamanı informasiyanın mühafizəsini təşkil etmək, məxfi məlumatların mühafizəsi tədbirlərinin icrasına nəzarət etmək üçün ümumi qanuni tələbləri müəyyənləşdirir.

Vurğulamaq lazımdır ki, əgər əlçatanlıq məhduddursa bu qanun ictimai və şəxsi məlumatları mühafizə obyekti kimi ayırmır. "İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında" Azərbaycan Respublikası Qanununun 2-ci maddəsi və Cinayət Məcəlləsinin 272-ci maddəsinin 1-ci hissəsində qeyd olunur ki, "informasiya - təqdim formasından asılı olmayaraq insanlar, əşyalar, faktlar, hadisələr, təzahürlər və proseslər haqqında məlumatdır".

Başqa sözlə, kompüter informasiyası kompüter mühitində yayılmış, kompüter qəbulu üçün əlçatan bir formada yazılmış və ya bir kompüterdən digərinə, kompüterdən periferik cihaza və ya cihazın idarəetmə sensoruna elektromaqnit siqnalları formasında telekommunikasiya kanalları vasitəsilə ötürülən bir məlumatdır.

Bununla yanaşı, cinayət hüququ sənədləşdirilmiş məlumatlar və onun digər növləri ilə birlikdə hüquqi müdafiəni təmin edir. Buna görə də cinayət fəaliyyəti subyektinin anlayışını genişləndirmiş olur. Hazırkı Azərbaycan Respublikasının Cinayət Məcəlləsinin təhlili göstərir ki, qanunverici kompüter müdafiəsi sahəsində yaranan münasibətləri xüsusi müdafiəyə aid olan informasiya münasibətlərinin bütün həcmindən ayırmışdır. Kompüter informasiyası sahəsində cinayətlər bölməsində əvvəllər yalnız cinayət hüquqi terminologiyasında deyil, həm də informasiya münasibətlərini tənzimləyən qanunvericilikdə terminlər və anlayışlar təqdim edilmişdir.

Azərbaycan Respublikasının mövcud cinayət qanunvericiliyi bizə aşağıdakı əsas nəticələrə gəlməyə imkan verir:

1. Azərbaycan Respublikası Cinayət Məcəlləsinin 271-273-cü maddələrində təsbit olunmuş normalar elmi mənbələrdə şərti olaraq kompüter cinayətləri adlandırılan ictimai təhlükəli hərəkətlərin bütün spektrini əhatə etmir. Daha dəqiq desək, ciddi nəticələrə səbəb olmaq məqsədi ilə kompüterin, kompüter sisteminin və ya onların şəbəkəsinin işləmə qaydalarının pozulmasına yönəldilmiş qəsdən əməllər Azərbaycan Respublikası Cinayət Məcəlləsinin 273-cü maddəsinin məzmunu ilə əhatə olunmur. Belə görünür ki, kimi, belə bir hərəkəti kompüter cinayətləri kateqoriyasına da aid etmək olar.

2. Kompüter cinayətləri kompüterin yalnız bir cinayət aləti deyil, cinayət törətmək üçün texniki vasitə hesab edildiyi cinayətlər də hesab olunur.

3. Kompüterin pozulma predmeti olduğu bütün halların kompüter cinayətləri kimi təsnif edildiyini də qəbul etmək olmaz. Azərbaycan Respublikası Cinayət Məcəlləsinin 271-273-cü maddələrində nəzərdə tutulmuş təsvir edilmiş kompozisiyalarda kompüterə hücum obyekti kimi yalnız müəyyən dərəcədə şərti olaraq baxıla bilər. Konvensiya bu vəziyyətdə təkcə maddi dünyanın bir obyekti kimi deyil, həm də informasiya və aparat təminatının birləşməsi kimi qəbul edilir. Cinayət hüququndakı cinayətin predmeti cinayətin törədildiyi şeydir (obyektiv maddi dünyanın subyekti). Cinayətin predmeti cinayət törətmək üçün alət və vasitələrdən fərqləndirilməlidir. Cinayət törətmək üçün texniki vasitə kimi kompüter, silah, vasitə, hər hansı bir texniki cihaz kimi vasitələrə baxılır. Bu mənada onun istifadəsi praktik əhəmiyyət daşıyır.

Beləliklə, kompüter cinayətlərində tək bir cinayət hücumu obyektini ayırd etmək demək olar ki, mümkün deyil. Cinayət hücumları obyektlərinin cinayət hüquqi müdafiəsi baxımından da çoxluğu var. Göründüyü cinayət kateqoriyasına yalnız avtomatlaşdırılmış məlumatların emalı sahəsində qanunsuz hərəkətlər aid

edilə bilər. Başqa sözlə desək, hücum obyekti kompüter sistemində işlənən məlumatdır və kompüter hücum vasitəsi kimi xidmət edir.

Virtual məkanda millətçilik Azərbaycan İnternet mühitinin müəyyənedici xüsusiyyətidir. Ermənistanla münasibətlərdəki siyasi böhran, həll olunmamış Dağlıq Qarabağ münaqişəsi hər iki tərəfin hakerləri arasında qarşıdurmaya səbəb oldu. 2008-ci ildən sonra Azərbaycanla Ermənistan arasındakı virtual qarşıdurma daha da kəskinləşdi. Bunun nəticəsində bir çox veb saytlar zərər gördü. Təbii ki, burada hədəf vacib milli qaynaqlar idi. Get-gedə hücumlar miqyas və koordinasiya etibarilə böyüməyə başladı. Cinayətkarlar isə tez-tez hücum üçün məsuliyyəti öz üzərilərinə götürərək hərəkətlərinə siyasi izahat verdilər. Hər iki tərəfdəki siyasətçilər veb saytlara qarşı vandalizm əleyhinə çıxış edərək, bunun "həll edilən" problemlərlə nisbətdə, hətta daha çox problem yaratdığını qeyd etdilər.

Bu tip hücumlara nümunə olaraq 2012-ci ilin avqustundan başlanan erməni hakerlər hücumlarını göstərmək olar. Bu zaman əsas hədəf kimi, Azərbaycanın əsas xəbər mənbələri, bir sıra rəsmi saytlar, o cümlədən Prezident Aparatı, Rabitə Nazirliyi və Ədliyyə Nazirliyinə aid saytlara müxtəlif növ hücumlar olmuşdur. Hücum azərbaycanlı zabit Ramil Səfərovun Macarıstandan ekstradisiyasına və dərhal əfv edilməsinə etiraz olaraq başladı. O, bir erməni zabitinin öldürülməsinə görə Macarıstanda ömürlük həbs cəzası çəkirdi. Nəticədə .am domenindəki bir neçə veb sayt, o cümlədən Ermənistan prezidentinin saytına hücumlar edildi.

İranlı və azərbaycanlı hakerlər də tez-tez veb saytlara bir sıra cavab hücumları ilə virtual döyüşlərdə iştirak edirlər. 2012-ci ilin yanvar ayında İranla əlaqəli olduğu iddia edilən bir qrup Azərbaycan Kiber Ordusu Bakı ilə Təl-Əviv arasındakı yaxın əlaqəyə etiraz olaraq təxminən 40 dövlət qurumuna hücum edərkən gərginlik artdı. Rabitə və İnformasiya Texnologiyaları Nazirliyi və Milli Təhlükəsizlik Nazirliyinin İnformasiya Təhlükəsizliyi şöbəsi bu hücumları araşdırdı və bildirildi ki, bu hücumların 25-dən 24-ü İrandan, biri isə Hollandiyadan həyata keçirilib. Buna cavab olaraq Pirates-ekipaj ("Pirates-crew") adlı azərbaycanlı haker qrupu İran saytlarına virtual hücum etdi. Azərbaycan

İnternet Forumunun rəhbəri Osman Gündüz, belə bir hücumun "müharibə zamanı baş verəcəyi təqdirdə virtual məkanımızı tamamilə məhv edəcəyi" xəbərdarlığını etdi. Gələcəkdə belə bir təhlükə bizi gözləyə bilər. "

Rejimi tənqid edən qəzetlərə yönəlmiş haker kiber hücumları 2013-cü il prezident seçkilərinə qədərki dövrdə də müşahidə edilmişdir. O dövrdə həm Azadlıq, həm də Müxbirlərin Azadlığı və Təhlükəsizliyi İnstitutu - RATİ belə hücumlar barədə məlumat verdi. Azadlıq veb saytının redaktoru Əli Rza qeyd edib ki, hakerlər tərəfindən veb saytda azad və ədalətli seçkilər üçün müxalifət nümayişinin təfərrüatlarını yerləşdirdikdən sonra veb sayta hücum olunub. RATİ rejimi aktiv şəkildə tənqid etdiyinə görə hakerlər üçün təbii bir hədəf halına gəlmişdir. Hücumların çoxu da azad və ədalətli seçki çağırışının nəticəsi hesab olunur.

İnformasiya emalının elmi və texniki vasitələrinin daim təkmilləşdirilməsi və daha da sürətlə inkişaf edən informasiya məkanının inkişafı şəraitində bəşəriyyətin növbəti əsrdə necə və harada olacağını çox çətinliklə təsəvvür edə bilərik.

3.2. Azərbaycanda informasiya təhlükəsizliyinin hüquqi tənzimlənməsi

Dövlət müstəqilliyinin bərpasından sonra Azərbaycan ictimai, siyasi və iqtisadi həyatın bütün sahələrində dinamik və sürətli inkişaf etməyə başlamışdır. Çox qısa bir zaman ərzində, hər bir sahədə uğurlu işlərə imza atılmış, qarşıya qoyulmuş məqsədə çatmaq üçün əhəmiyyətli addımlar atılmışdır. Burada neft və qeyri-neft sektorunun, özəl sektorun, biznes və sahibkarlıq mühitinin adını qürurla çəkmək olar. Azərbaycanda hökm sürən sabitlik və ictimai-siyasi nizam öz növbəsində informasiyalaşdırma sahəsində də mühüm addımların atılmasına imkan verdi.

Bu sahədə xüsusi olaraq, 1995-ci ildə ümumxalq səsverməsi (referendum) ilə qəbul edilmiş Azərbaycan Respublikasının Konstitusiyası qeyd etmək lazımdır.

Çünki Konstitusiyanın qəbulu təkcə qanunverici baza kimi normaları müəyyənləşdirmədi, o həmçinin, informasiya qanunvericiliyinin inkişafında da çox əhəmiyyətli hadisə oldu. Qəbul edilmiş Konstitusiyanın 50-ci maddəsinə əsasən hər kəs qanuni yolla əldə etmək, ötürmək, istehsal etmək və yaymaq hüququna malik idi. Məhz təkcə bu maddənin informasiyanın gücünü və təsir dairəsini izah etməkdə nə qədər güclü bir ifadə vasitə olduğunu görmək olur.

İnformasiya qaynaqlarının formalaşması və istifadəsi zamanı yaranan hüquqi münasibətləri tənzimləmək üçün 1998-ci ildə daha bir qanunun qəbul edilməsi zərurəti yarandı. Beləliklə, 1998-ci ilin 3 aprel tarixində "İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında" Azərbaycan Respublikasının Qanunu qəbul olundu. Bu Qanun təkcə informasiyalaşdırma sahəsində yaranan hüquqi münasibətləri deyil, həm də informasiyanın mühafizəsi, informasiya proseslərində və informasiyalaşdırma ilə məşğul olan subyektlərin hüquqlarını tənzimləyirdi.

1999-cu ilin 7 dekabr tarixində bu sahədə daha bir böyük addım atıldı və "Kütləvi informasiya vasitələri haqında" Qanun qəbul edildi. Bu qanun Azərbaycan Respublikasında kütləvi informasiyanın axtarışı, əldə olunması, hazırlanması, ötürülməsi, istehsalı və yayımı haqqında ümumi qaydaları müəyyənləşdirir. Qanun özündə mətbuatın, televiziya-radio təşkilatlarının, informasiya agentliklərinin vətəndaşların tam, doğru və operativ informasiya almaq hüququnun həyata keçirilməsinə yönəldilmiş fəaliyyətinin təşkilati, hüquqi və iqtisadi əsaslarını birləşdirir.

Sonrakı dövrdə 2004, 2005, 2008, 2009, 2011-ci illərdə müvafiq olaraq, "Elektron imza və elektron sənəd haqqında" Qanun, "Elektron ticarət haqqında" Qanun, "Biometrik informasiya haqqında" Qanun, "Kibercinayətkarlıq haqqında" Konvensiyanın Təsdiq edilməsi barədə Qanun və "Fərdi məlumatlar haqqında" Qanun imzalanmış və qüvvəyə minmişdir. Bütün bu qanunlar İnformasiya-Kommunikasiya texnologiyaları sahəsində yaradılmış hüquqi aktlar olaraq, bu sahənin davamlı diqqət mərkəzində olmasına gətirib çıxarmışdır.

Qeyd etmək lazımdır ki, müasir cəmiyyətin heç bir sahəsi inkişaf etmiş bir informasiya quruluşu olmadan fəaliyyət göstərə bilməz. Milli informasiya resursu bu gün dövlətin əsas güc mənbələrindən biri hesab olunur. Dövlətin fəaliyyətinin bütün sahələrinə nüfuz edən informasiya artıq konkret siyasi və maddi dəyər kimi əhəmiyyət kəsb edir. Bu fonda ölkənin milli təhlükəsizliyinin ayrılmaz bir elementi kimi informasiya təhlükəsizliyini təmin etmək vəzifəsi getdikcə aktuallaşır və informasiyanın mühafizəsi prioritet dövlət vəzifələrindən birinə çevrilir. İnformasiyanın mühafizəsi istənilən dövlətdə təmin edilir və onun inkişafı dövlətin ehtiyaclarından, onu əldə etmək imkanlarından, metod və vasitələrindən, dövlətin hüquqi rejimindən və onu təmin etmək üçün real səylərdən asılı olaraq bir çox mərhələlərdən keçir.

İnformasiyalaşdırma müasir cəmiyyət həyatının xarakterik xüsusiyyətinə çevrilib. Dünya təcrübəsi göstərir ki, İKT-nin geniş yayılması ölkənin hərtərəfli inkişafına səbəb olur. Beləki, yeni informasiya texnologiyaları xalq təsərrüfatının bütün sahələrində fəal şəkildə tətbiq olunur. İKT-nin tətbiqi səviyyəsi intellektual və elmi potensialın, dövlət idarəçiliyində şəffaflığın və demokratiyanın əsas göstəricisidir. Cəmiyyətin əsas sahələri üçün potensial inkişaf imkanları informasiya proseslərinin vəziyyəti ilə müəyyən edilir. Hal-hazırda informasiya ölkənin əsas sərvətlərindən biri kimi strateji milli sərvət hesab olunur.

Beynəlxalq və dövlətlərarası münasibətlərdə hər bir ölkənin ictimai-siyasi və sosial-iqtisadi inkişafının əsas istiqamətlərindən biri də məhz dünya birliyinə inteqrasiyadır. Bu gün milli sərhədlər cəmiyyətin müxtəlif sahələrində inteqrasiyanın atributlarının qlobal inkişafına maneə olmur. İnformasiyalaşdırma qloballaşmanın yayılması üçün ən vacib və zəruri şərtlərdən biri hesab olunur. Bu proseslərin obyektiv, şəffaf və effektiv şəkildə idarə olunması isə dövlət tərəfindən tənzimlənən milli qanunvericilik və hüquq-mühafizə tədbirləri ilə təmin olunur.

Cəmiyyətin informasiya sistemlərinin vəziyyəti və onların hüquqi müdafiəsi dərəcəsi dövlətin qlobal proseslərə inteqrasiyası üçün bir meyar kimi qiymətləndirilir. Dövlətin beynəlxalq tənzimləmə standartlarına əməl etməsi

cəmiyyətin mövcud dünya nizamına və dövlətin özünə xələl gətirmədən informasiya və rabitə texnologiyalarından istifadəsinin hüquqi səviyyəsini və qoruyucu təminatlarını səciyyələndirir. İnformasiya təhlükəsizliyi sistemlərində "informasiya" və "qanun" anlayışları əsas yer tutur. İnformasiya təhlükəsizliyi dedikdə, informasiya sahəsində fərdin, cəmiyyətin və dövlətin balanslaşdırılmış maraqlarının qorunması vəziyyəti başa düşülür [10].

Müasir qloballaşmanın əsas amillərindən biri kimi geosiyasi subyektlərin təcrid olunmasının zəifləməsini misal göstərmək olar. Bu da İKT əsasında qarşılıqlı münasibətlərinin yaranmasına və inkişafına şərait yaradır. Sürətlə inkişaf edən elmi-texnoloji tərəqqi, informatika və kibernetika təkcə texnoloji deyil, həm də sosial, iqtisadi və siyasi prosesləri sürətləndirir.

Beynəlxalq məkanda hər bir dövlət üçün ayrıca informasiya təhlükəsizliyinin hüquqi təminatı problemini həll etmək üçün əlaqələndirilmiş beynəlxalq tədbirlərə ehtiyac duyulur. 2013-cü ilin iyununda Böyük 8-lik ölkələrinin (ABŞ, Rusiya, Birləşmiş Krallıq, Kanada, Yaponiya, Almaniya, Fransa, İtaliya) iclasında qəbul edilmiş "Açıq Məlumat Xartiyası", əvvəllər Okinavada elan edilmiş "hamı üçün və sərhədsiz informasiya" ideyasını inkişaf etdirmiş və milli informasiya qaynaqlarının formalaşması və onların qlobal formatda yaxınlaşması üçün müəyyən tövsiyələr vermişdir.

Beynəlxalq tövsiyələr və hüquqi öhdəliklərlə asanlaşdırılan dövlətlərin milli təhlükəsizlik siyasətində və strategiyalarında bütün bu çağırışlar öz əksini tapmalıdır. Bütün demokratik inkişaf etmiş ölkələrdə olduğu kimi, Azərbaycan Respublikasının da informasiya təhlükəsizliyinin təmin edilməsi sahəsində dövlət siyasəti beynəlxalq hüquqa uyğun institusional mühitin və qanunvericilik bazasının yaradılması ilə əlaqəli konseptual tədbirlərdən ibarətdir.

90-cı illərin ortalarında Azərbaycan Respublikasında siyasi, elmi və texniki sahələrdə keyfiyyətcə dəyişikliklər baş verdi. Bu da ümumilikdə informasiyanın mühafizəsi sahəsində dövlət siyasətinə yenidən baxılma məsələsini gündəmə

gətirdi. İnformasiya texnologiyası onun ötürülməsi və emalı texniki vasitələrində dövriyyədə olan informasiyanın həcmini və əhəmiyyətini əsaslı şəkildə dəyişdirdi. İnformasiya sahəsində milli maraqlar vətəndaşların informasiya almaq və istifadə sahəsində konstitusiya hüquq və azadlıqlarına riayət etmək, müasir telekommunikasiya texnologiyalarının inkişafı, dövlət informasiya ehtiyatlarının icazəsiz girişdən mühafizəsidir.

Azərbaycanın hüquqi bazası çox vaxt Sovet dövrünün qanunlarının "qalıqları" kimi qəbul edilir. Lakin, bu fikir kifayət qədər dayaz düşüncələrin məhsulu sayıla bilər. Çünki, İKT-ə ayrılan dövlət qayğısı Sovet dövrü ilə müqayisə olunmayacaq dərəcədə yüksək səviyyədədir. Dövlət ölkənin əsas operatoru olan Delta Telecom beynəlxalq əlaqələrin böyük hissəsini idarə edən və yeganə internet trafik mübadiləsi məntəqəsini idarə edən ən böyük topdansatış internet provayderi ilə sıx əlaqə saxlamaqla İKT sektoruna təsirini həyata keçirir. 2014-cü ilin mart ayının əvvəlində Rabitə və Yüksək Texnologiyalar Nazirliyi (RYTN) adını alan nazirlik hazırda İKT sahəsində əsas tənzimləyici orqandır və 2005-ci il Rabitə haqqında Azərbaycan Respublikasının Qanununa uyğun olaraq fəaliyyət göstərir.

RYTN dövlət səviyyəsində yüksək səviyyəli bir domenin təşkili və yerləşdirilməsi, telekommunikasiya fəaliyyətinin lisenziyası, operatorlar arasında qarşılıqlı əlaqələri tənzimləyən və ümumiyyətlə rəqabətli və inhisarçı İKT mühitini təşviq edən bir qərar vermişdir. Bununla belə, birinci dərəcəli provayderlərin mülkiyyətində dövlət payının olması onun RYTN-nin antiinhisar İKT mühitinin stimulyatoru kimi işləməsi qabiliyyətini sual altına alır. Məsələn, bir anda RYTN hökumət əlaqələri olan bir təşkilat olan Azerfon-a Azərbaycanda 3G şəbəkəsindən istifadəyə müstəsna hüquqlar vermişdir. [12]

Azərbaycanda RYTN ölkədə interneti məhdudlaşdırmaq, dəyişdirmək və izləmək üçün xeyli gücə malikdir. İnternet provayderləri ilə hakimiyyət orqanları arasındakı əlaqələri nəzərə alaraq, Bakı İKT sektoruna nəzarəti həyata keçirmək üçün qeyri-rəsmi və cavabdeh olmayan bir mexanizmlə təmin edilmişdir.

Fövqəladə Qanun RYTN-ə fövqəladə hal və ya təbii fəlakət olduqda abunəçiləri xəbərdar etmədən seçilmiş şəbəkələrdən istifadə hüququ da verir.

Bundan əlavə, "İnternet xidmətlərindən istifadə qaydaları"na uyğun olaraq, RYTN və özəl operatorlar 2005-ci il "Telekommunikasiya haqqında" Qanunu pozduğu hallarda abunəçiləri xəbərdar etmədən İnternet xidmətlərinin dayandırılmasını tələb edə bilərlər. Qaydalarda, eyni zamanda, abunəçinin səlahiyyətli tərəflərə mənfi təsir göstərən onlayn məlumat yerləşdirdiyi hallarda provayderin internet xidmətlərini müvəqqəti olaraq dayandıra biləcəyi də göstərilir. Qaydalar həm də provayderlər və istifadəçilər arasındakı münasibətləri tənzimləyir. Nəzəri baxımdan belə tənzimləmə istehlakçını qorumalı olsa da, əslində bir növ minimum xidmət standartı və ya şəbəkə bitərəfliyini qorumağın hüquqi yollarını təmin edən rəsmi bir mexanizm yoxdur.

Media Qanununun 10-cu maddəsi medianın, o cümlədən internetin təbliğat və sui-istifadə, etnik, irqi, sosial ziddiyyətləri və ya tolerantlığın olmaması və ya digər qeyri-qanuni hərəkətləri təşviq etmək üçün istifadəsini cinayət sayır. Bu yanaşma problemlidir və o deməkdir ki, bütün onlayn məzmun ənənəvi media ilə eyni qaydaların və məhdudiyyətlərin potensial obyekti ola bilər. 2010-cu ildə mətbuatı təmsil etmək üçün 2003-cü ildə yaradılan dövlət tərəfindən idarə olunan Mətbuat Şurası peşəkar jurnalistika qaydalarına riayət etmək məqsədi ilə yeni saytların monitorinqinə başlayacağını elan etdi. Bu səlahiyyətləri tənzimləmək üçün 2013-cü ilin fevral ayında onlayn mühitdə etik pozuntularla bağlı iddialarla işləmək üçün xüsusi bir komissiya da yaradıldı.

RYTN naziri və Milli Televiziya və Radio Şirkətinin naziri provayderlərin, veb saytların və kommersiya onlayn xidmətlərinin RYTN-də qeydiyyatdan keçmələrini və informasiya təhlükəsizliyini təmin etmək üçün lisenziyalar əldə etmələrini təklif etdi (Azərbaycan Cinayət Məcəlləsinin 283-cü maddəsi milli, irqi, sosial və ya dini nifrət və ya düşmənçilik və ya milli ləyaqəti alçaldan, vətəndaşların hüquqlarını məhdudlaşdırmaq və ya milli, irqi və ya sosial vəziyyət

və ya dinə münasibət əsasında vətəndaşlar arasında üstünlük yaratmaq məqsədi daşıyan hərəkətlər.).

Beynəlxalq birliyin Azərbaycan Cinayət Məcəlləsində və Media haqqında qanunda əks olunan böhtan xarakterli məlumatların yayılması haqqında bəndin qaldırılmasına cəhd göstərməsinə baxmayaraq, o, hələ də cinayət tərkibi olaraq qalır. Dövlət internetdə böhtan xarakterli məlumatların yayılmasına görə cinayət məsuliyyətinin sahəsini də genişləndirib. 2013-cü ilin may ayında Cinayət Məcəlləsinin 147 (böhtan) və 148 (təhqir) maddələrinə düzəlişlər edildi. Bu hal yalan hesab edildiyi təqdirdə isə sosial şəbəkələrdə öz fikirlərini və ya tənqidlərini ifadə etdiyi üçün 3 il müddətinə azadlıqdan məhrumetmə ilə cəzalandırılır. Məhkəmə qərarı olmadan "inzibati" həbs cəzalarının da maksimal cəzası 15 gündən üç aya qədər artırıldı.

Bəzi hallarda böhtan xarakterli məlumatların və böhtanların yayılması ilə bağlı hüquq-mühafizə orqanlarının, o cümlədən bloqqerlər və onlayn müxalifətçilərin mediaya qarşı təcavüz etdiyi, həbs olunduğu və mühakimə olunduğu hallara rast gəlinir. Hökümət orqanları ilə sıx əlaqəli bir bankın keçmiş işçisi Mikayıl Talıbov özünün Facebook səhifəsində keçmiş işəgötürən AccessBank haqqında təhqiramiz şərhlər yerləşdirdi və hətta onu "Ədalətsiz Bank" ("Ədalətsizlik Bankı") adlandırmağa belə getdi. İnternetdəki duyğularının artması nəticəsində Talıbov bir il islah işləri və illik maaşının 20 faizi cərimə cəzasına məhkum edildi. 2011-ci ilin may ayında hökumət yalan məlumatların yayılmasını kiber cinayət kimi təsnif etdi.

İnternetdə təşkil olunan etiraz aksiyalarının sayının və miqyasının artması ikinci və üçüncü nəsillərin təsirli texnikası olan kütləvi toplaşmalar haqqında qanunun sərtləşməsinə səbəb oldu. Bu da siyasi etirazların virtual məkandan küçələrə çıxmasının qarşısını almağa kömək etdi. Yeni qanun icazəsiz iclaslar üçün cəriməni maksimum 3800 dollar həddinə qədər artırdı. Orta əmək haqqının ayda cəmi 400 dollar olduğunu nəzərə alsaq, bu çox böyük məbləğdir. Artıq bu qanunlar diqqətlə tətbiq olunur. Belə ki, 2012-ci ilin yanvarında Bakının mərkəzində

keçirilən və ordu sıralarına yeni qəbul olunanların rəftarına qarşı təşkil olunan etiraz aksiyası zamanı 22 nəfər həbs edilmişdi. Qeyd edək ki, bu etiraz demək olar ki, bütünlüklə sosial şəbəkələr vasitəsilə təşkil edilmişdi.

Azərbaycan Respublikasında informasiya təhlükəsizliyinin təmin edilməsinin ən vacib vəzifələri bunlardır:

- informasiya fəaliyyəti sahəsində vətəndaşların konstitusiya hüquq və azadlıqlarının həyata keçirilməsi;
- informasiya infrastrukturunun təkmilləşdirilməsi və mühafizəsi, qlobal informasiya məkanına inteqrasiya;
- informasiya sahəsindəki qarşıdurma təhlükəsi ilə mübarizə.

İnformasiya sferasında milli maraqların əsasən, dörd əsas komponenti olur.

Birinci komponentə informasiyanın əldə edilməsi və istifadəsi, mənəvi yenilənmə, cəmiyyətin mənəvi dəyərlərinin, vətənpərvərlik və humanizm ənənələrinin, ölkənin mədəni və elmi potensialının qorunması və möhkəmləndirilməsi sahəsində insan və vətəndaşın konstitusiya hüquq və azadlıqlarına riayət olunması daxildir.

İkinci komponentə dövlət siyasəti haqqında etibarlı informasiyanın beynəlxalq ictimaiyyətə çatdırılması, beynəlxalq həyatda baş verən ictimai əhəmiyyətli hadisələrə rəsmi mövqeni və vətəndaşların açıq dövlət informasiya ehtiyatlarına çıxışı ilə bağlı dövlət siyasətinin informasiya dəstəyi daxildir.

Üçüncü komponent müasir informasiya texnologiyalarının, informasiya sənayesinin, o cümlədən informasiyalaşdırma vasitələri, telekommunikasiya və rabitə sənayesinin inkişafı, daxili bazarın öz məhsulları ilə tələbatını ödəmək və bu məhsulların dünya bazarına çıxması, eyni zamanda, informasiya ehtiyatlarının yığılmasını, mühafizəsini və səmərəli istifadəsini təmin etməkdir. Bu gün yalnız bu əsasda yüksək texnologiyaların yaradılması, sənayenin texnoloji yenidən qurulması və elm və texnikanın nailiyyətlərini bir araya gətirmək problemlərini həll etmək mümkündür.

Dördüncü komponent informasiya mənbələrini icazəsiz girişdən qorumaq, həm quraşdırılmış, həm də yeni yaradılan ərazidəki informasiya və telekommunikasiya sistemlərinin təhlükəsizliyini təmin etməkdir. Son illərdə Azərbaycanda informasiya-kommunikasiya texnologiyalarının tətbiqi sahəsində bir sıra addımlar atılmış, bu sahə dövlət siyasətinin ən yüksək prioritetlərindən birinə çevrilmişdir.

Qeyd etmək lazımdır ki, bir çox ölkələrdə informasiya ehtiyatlarında de-fakto dövlət inhisarı vətəndaşa informasiya axtarmaq, almaq və yaymaq üçün konstitusiya ilə müəyyən edilmiş hüquqlar verir.

"İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında" AR Qanununun 18-ci maddəsində də informasiyanın mühafizəsinin əhəmiyyəti vurğulanır. “Dövlət sirri haqqında” Azərbaycan Respublikasının Qanunu isə informasiyanın dövlət sirri kimi təsnifatı, gizlədilməsi və mühafizəsi ilə əlaqədar yaranan münasibətləri, ölkənin təhlükəsizliyinin təmin edilməsi baxımından tənzimləyir.

İnformasiya təhlükəsizliyi aşağıdakıların qarşısını almaqla təmin edilməlidir:

- Məlumatların sızması, oğurlanması, itirilməsi, təhrif edilməsi, saxtalaşdırılması;
- Fərdin, cəmiyyətin və dövlətin təhlükəsizliyinə yönəlmiş təhdidlər;
- İnformasiyanı silmək, dəyişdirmək, təhrif etmək, surəti çıxarmaq, bloklamaq üçün icazəsiz tədbirlər;
- Vətəndaşların şəxsi sirlərini və informasiya sistemlərində mövcud olan fərdi informasiyaların məxfiliyini qorumaq üçün konstitusiya hüquqlarını qorumaqla sənədləşdirilmiş məlumatların mülkiyyət obyekti kimi hüquqi rejimini təmin edərək informasiya mənbələrinə və informasiya sistemlərinə qanunsuz müdaxilənin digər formaları. .

Bununla birlikdə, "İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında" AR Qanunu fərdi məlumatlarına daxil olmaq hüquqlarının

qorunması və istifadə zamanı şəxslərin inzibati və hüquqi statusunun müəyyənləşdirilməsində və şəxsin hüquqi rejiminin təmin edilməsində bu məlumatların mühafizəsinə dair müddəanı nəzərə almır.

Xüsusi vurğulayırıq ki, əhaliyə informasiya və psixoloji təsir göstərən əsas aparıcı olan dövlət və qeyri-hökumət qurumları və kütləvi informasiya vasitələri, digər ölkələrin rəhbərliyi geosiyasi fəaliyyətin informasiya dəstəyi vasitəsinə çevrilməlidir.

Bir daha qeyd etmək lazımdır ki, bütün inkişaf etmiş ölkələr ictimai həyatın əsas sahələrində informasiya texnologiyalarının istifadəsinə dair dövlət proqramları formalaşdırır. Bu, ilk növbədə elektron ticarətin xidmətinə, idarəetmənin elektronlaşdırılmasına, təhsil, mədəniyyət və media sahələrində informasiya texnologiyalarının geniş yayılmasına aiddir. Ancaq ən kəskin məsələ dövlət strukturlarında informasiya texnologiyalarından istifadənin geriləməsidir. Məsələ tək bir işçiyə düşən kompüterlərin sayında deyil. Fakt budur ki, açıq sistemlərdəki kompüterlərin əksəriyyəti hələ də vahid şəbəkələrə qoşulmur və elektron sənədlərə və müasir sənəd idarəçiliyinə aktiv keçidi təmin etmir. İcra orqanlarının qanunu və siyasəti hələ bu sahədə lazımi yenilikləri təmin etmir.

İnformasiya təhlükəsizliyinin tənzimlənməsi, informasiya sahəsində milli maraqların dörd əsas komponentinə əsaslanır:

- Fərdi məlumatların və şəxsi sirrlərin təminatına əməl edilərkən vətəndaşın informasiya almaq və ondan istifadə sahəsində hüquq və azadlıqlarına riayət edilməsi;
- Dövlət siyasətinin informasiya təminatı, cəmiyyətin, dövlətin və fərdin maraqlarının tarazlığını təmin edərkən dövlət siyasəti haqqında etibarlı məlumatların formalaşdırılması;
- Modern müasir informasiya texnologiyalarının, informasiya və informasiyalaşdırma vasitələri, rabitə və rabitə sənayesinin inkişafı, bu növ məhsullar üçün bazarın formalaşdırılması;

- İnformasiya mənbələrini icazəsiz girişdən qorumaq, informasiya və telekommunikasiya sistemlərinin təhlükəsizliyini təmin etmək.

Bu sahələrin hər biri yalnız qanuni vasitə və metodların köməyi ilə deyil, texnoloji bazaya söykənən böyük təşkilati iş prosesində həll edilməli olan xüsusi tapşırıqlarla doldurulmuşdur. Qanuni tənzimləmə və informasiya təhlükəsizliyinin təmin edilməsi sahəsinin spesifikliyi, ümumilikdə informatika sahəsinin inkişafı üçün təhlükəsiz şəraitin təmin edilməsi üçün profilaktik və birbaşa işlər arasında tarazlığın olmasıdır. Bu mərhələdəki boşluqlar və ya ziddiyyətlər informasiyalaşdırma sisteminin özündən, informasiya məhsulları və xidmətlərinin istehlakçılarının mühitindən yaranan təhdidlərə səbəb olur.

NƏTİCƏ VƏ TƏKLİFLƏR

"İnformasiya təhlükəsizliyinin hüquqi tənizimlənməsində beynəlxalq təcrübə və onun Azərbaycanda tətbiqi" mövzusunun tədqiqi zamanı aşağıdakı yekun nəticələr əldə edilmişdir:

Azərbaycanda informasiya təhlükəsizliyinin təmin olunması sahəsində uğurlu siyasət tətbiq olunur. Ölkəmizdə daim inkişaf etdirilən milli strategiya formalaşdırılmış və bu strategiyada İKT-nin inkişafına, informasiya sistemlərinin (İS) təhlükəsiz və sərbəst fəaliyyətinə, xüsusilə də, təhlükəsizlik məsələlərinə böyük diqqət və qayğı göstərilmişdir. İnformasiya təhlükəsizliyinin təmin olunmasının əsas istiqamətlərindən olan hüquqi tənzimləmələr də diqqətdən kənar qalmamış, bu sahədə yeni qanunvericilik bazası da formalaşdırılmışdır.

Dissertasiya işində təhlükəsizliyin hüquqi tənzimlənməsinə yönəlmiş müxtəlif ölkələrin fərqli yanaşmalarının üstün cəhətləri, çatışmazlıqları, hal-hazırda istifadə edilən hüquqi aspektlərin ən vacib funksiyaları və xarakteristikaları geniş tədqiq edilmişdir.

Dissertasiya işində, həmçinin, təhlükəsizliyin tənzimlənməsində beyəlxalq təcrübədən də geniş bəhs olunur. Belə təcrübənin formalaşması uzun bir müddət ərzində baş verdiyindən, ayrı-ayrı tarixi hadisələrin də ona təsiri danılmazdır. Məhz bu təsir nəticəsində də tənzimləmələr zaman keçdikcə daha da təkmiləşmiş və müasir halını almışdır.

Tədqiqat işində müxtəlif ölkələrdə təhlükəsizlik üçün yaradılan qanunvericilik bazasının praktiki və nəzəri cəhətləri müzakirə edilir. Dissertasiya işinin ən əsas məqsədi Azərbaycanda informasiya təhlükəsizliyinin hüquqi tənzimlənməsi üçün görülən tədbirlərin geniş şərhini vermək və onların cari dövrdə aktuallığını müzakirə etməkdir.

Burada əsas diqqət qanunverici baza olan Azərbaycan Respublikası Konstitusiyasında təhlükəsizlikliklə bağlı olan maddələrə, KİV bu barədə araşdırmalarına yönəldilir.

Aparılan tətdiqat nəticəsində aşağıdakılar müəyyən edilmişdir:

1. Hal-hazırda bütün dünyada informasiya təhlükəsizliyi məsələsi aktual mövzu olmaqla yanaşı, daim inkişafda olan bir mövzu kimi də diqqət mərkəzindədir. Davamlı olaraq bu sahədə keçirilən seminarlar, konfranslar təkmilləşməyə təkan verən əsas amillərdəndir.

2. Azərbaycan hökuməti bu sahəni prioritet sahələrdən biri seçməklə onun inkişafına xüsusi diqqət göstərdiyini vurğulayır. Bu mənada son 10 il mühüm əhəmiyyətə malik illər sayıla bilər. Belə ki, yeni Cinayət Məcəlləsinin müvafiq bəndləri cinayətkara ən ağır cəzanın verilməsini tələb edir. Bu da informasiya təhlükəsizliyinin pozulmasının böyük fəsadlara gətirib çıxaracağına işarədir.
3. Bu sahəyə böyük diqqət və qayğı yönəlməsinə, hüquqi tənzimləmələrin kifayət qədər sərtləşdirilməsinə baxmayaraq, hələ də müəyyən qədər risk ehtimalı qalmaqdadır. Buna görə də, fərdi şəxsdən tutmuş nəhəng müəssisə və şirkətlərə qədər hər kəs öz məlumatlarının mühafizəsinə görə müəyyən qədər, istər proqram təminatı səviyyəsində, istərsə də texniki səviyyədə tədbirlər görməli və buna ciddi yanaşmalıdır.

İnformasiya təhlükəsizliyi bütün dövrlərdə bu və ya digər formada xüsusi əhəmiyyətli problemlərdən sayılıb. Hələ ən qədim dövrlərdən bəri fərdi və ya dövlət əhəmiyyətli informasiyanın ələ keçməməsi üçün yalnız göndərən və ya alıcı tərəfindən açıla bilən xüsusi növ şifrələmələrdən, kriptoqrafik üsullardan istifadə olunub. Təbii ki, zaman keçdikcə istər bu üsullar, istərsə də digər növ tədbirlər inkişaf edərək daha geniş sahəyə yayılmağa başladı.

İnformasiya təhlükəsizliyi məsələsi XX əsrin ortalarından etibarən dünya ölkələrini bu mövzu ətrafında birləşdirməyə başladı. Tezliklə bu mövzuda beynəlxalq seminarlar, konfranslar keçirilməyə başladı. Bu konfransların məntiqi nəticəsi olaraq isə hüquqi baza formalaşmağa başladı. Hüquqi tənzimləmələr bütün ölkələr arasında informasiya prosesləri zamanı təhlükəsizliyin təmini olunması üçün mühüm əhəmiyyət kəsb edir.

İSTİFADƏ OLUNMUŞ ƏDƏBİYYAT SİYAHISI

1. Əlizadə Mətləb Nuruş oğlu, Bayramov Hafiz Məhərrəm oğlu, Məmmədov

Əlövsət Suliddin oğlu, İnformasiya təhlükəsizliyi, Dərslik, Bakı, "İQTİSAD UNİVERSİTETİ" nəşriyyatı, 2016, 384 səh.

2. Mozanlı İlham Abbas oğlu, Söz azadlığı və informasiya təhlükəsizliyi: milli və beynəlxalq təminat, Bakı: UniPrint, 2005, 160 səh. [12]
3. Qasımov Vaqif Əlicavad oğlu, İnformasiya təhlükəsizliyi: kompüter cinayətkarlığı və kiberterrorçuluq, Bakı: Elm, 2007, 192 səh. [4]
4. "İnformasiya təhlükəsizliyinin aktual problemləri" III respublika elmi-praktiki seminarının əsərləri, Bakı, 2017, 130 səh. [8]
5. Мельников Владимир Павлович, Информационной безопасность и защита информации, Москва: Academia, 2006, 330 с.
6. Arihant Khicha, Neeti Kapoor, İnformation system security, Genius Publication, 2016, 455 pages [7]
7. Richard E. Smith, Elementary information security, Jones&Bartlett Publishers, 2015, 866 pages
8. Timothy P.Layton, İnformation security: Design, İmplementation, Measurement and Compliance, CRC Press, 2016, 264 pages. [9]
9. Enes Aslanbakan, Bilgi güvenliği ve uygulamalı hacking yöntemleri, Pusula yayıncılık, 2016, 148 sayfa
10. Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Bakanlar Kurulu Kararı (20.10.2012 tarih, 28447 sayılı T.C. Resmi Gazete)
11. https://www.wipo.int/edocs/lexdocs/laws/az/az/az018az.pdf [10]
12. https://cert.az/news/2016/informasiya-tehlukesizliyi-ve-ona-qarsi-yonelmis-hucumlar
13. https://ict.az/uploads/konfrans/info_sec/RS08_INFORMATION-SECURITY-IN_AZERBAIJAN-IN-THE-CONTEXT-OF-NATIONAL-INTERESTS.pdf
14. https://searchinform.ru/informatsionnaya-bezopasnost/osnovy-ib/ugrozy-informatsionnoj-bezopasnosti/ [3]
15. https://studme.org/78404/pravo/pravovoe_regulirovanie_informatsionnoy_bezopasnosti_sisteme_rossiyskogo_informatsionnogo_prava [6]

16. http://www.advertology.ru/index.php?name=Subjects&pageid=195
17. https://lawbook.online/kniga-grajdanskoe-pravo-rossii/pravovoy-rejim-zaschityi-gosudarstvennoy-20781.html
18. https://zaochnik.com/spravochnik/pravo/organizatsionno-pravovoe-obespechenie-informatsion/pravovoe-regulirovanie-informatsionnoj-bezopasnost/
19. https://pirit.biz/reshenija/informacionnaja-bezopasnost
20. https://www.geeksforgeeks.org/what-is-information-security/ [1]
21. https://www.intechopen.com/online-first/legal-aspects-of-international-information-security [5]
22. http://www.oecd.org/sti/ieconomy/49338232.pdf [11]
23. https://www.springer.com/gp/book/9783319998060
24. https://www.techopedia.com/definition/24838/information-security-policy
25. https://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-program/resources/information-security-guide/security-policies/information-security-policy-examples
26. https://www.exabeam.com/information-security/information-security-policy/
27. https://searchsecurity.techtarget.com/definition/information-security-infosec
28. https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security
29. https://www.researchgate.net/publication/279679417_Information_Security_Standards
30. http://www.egisbilisim.com.tr/bilgi-guvenligi-alanindaki-hukuki-duzenlemeler/
31. http://www.bilgitoplumu.gov.tr/wp-content/uploads/2015/11/Ulusal_Bilgi_Guvenligi_Strateji_ve_Kurumsal_Yapilanma.pdf [2]
32. http://blog.normaturk.com/bilgi-guvenligi-nedir/
33. http://www.bilgimikoruyorum.org.tr/?b122_bilgi-guvenliginden-kim-sorumludur
34. https://www.btyon.com.tr/iso-27001-belgesi.php

35. http://yunus.hacettepe.edu.tr/~sadi/yayin/INTET2016_Tuluk-Seferoglu_Ulusal-UA-Bilgi-G%C3%BCvenligi-Politikalari.pdf
36. http://www.yasad.org.tr/tr/Sayfa/ulusal-bilgi-guvenligi-kanun-tasarisi

Р Е Ф Е Р А Т

Информационная безопасность всегда была одной из самых важных проблем в той или иной форме. С древних времен для предотвращения

захвата личной или общедоступной информации использовались специальные типы шифрования и криптографические методы, которые могут быть расшифрованы только отправителем или получателем. Конечно, со временем эти методы, как и другие виды мер, развивались и стали распространяться.

Вопрос информационной безопасности начал объединять страны мира вокруг этой темы в середине двадцатого века. Международные семинары и конференции по этой теме вскоре стали проводиться. Как логичный результат этих конференций, правовая база начала формироваться. Правовые нормы важны для обеспечения безопасности во время информационных процессов между всеми странами.

В нашей области проделана большая работа в этой области, проведены успешные реформы в области законодательства. Хотя с момента обретения независимости прошло очень мало времени, в области ИКТ достигнуты большие успехи. В частности, объявление 2013 года «Годом информационных и коммуникационных технологий» в Азербайджанской Республике можно считать ярким примером внимания и заботы, уделяемых этой области.

При подготовке диссертации была детально изучена динамика развития в области правового регулирования в Азербайджане, проведено сравнение прошлого и настоящего в этой области, для этого использованы различные местные и зарубежные книги и информация, полученные через Интернет. Исследования многих авторов в этой области, а также интернет-ресурсов, были рассмотрены.

S U M M A R Y

Information security has always been one of the most important problems in one form or another. Since ancient times, special types of encryption and cryptographic methods, which can only be decrypted by the sender or recipient, have been used to prevent the seizure of personal or public information. Of course, over time, these methods, as well as other types of measures, developed and began to spread.

The issue of information security began to unite the countries of the world around this topic in the middle of the twentieth century. International seminars and conferences on this topic were soon held. As a logical result of these conferences, the legal framework began to take shape. Legal regulations are important to ensure security during information processes between all countries.

Great work has been done in this area in our country, and successful reforms have been carried out in the field of legislation. Although very short time has passed since independence, great strides have been made in the field of ICT. In particular, the announcement of 2013 as the "Year of Information and Communication Technologies" in the Republic of Azerbaijan can be considered a clear example of the attention and care paid to this area.

During the preparation of the dissertation, the dynamics of development in the field of legal regulation in Azerbaijan was studied in detail, the past and present of this field were compared, various local and foreign books and information obtained via the Internet were used for this purpose. Research by many authors in this area, as well as Internet resources, has been reviewed.